IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

| | | |
|---|---|---|
| CENTRIPETAL NETWORKS, INC., | ) | |
| | ) | |
| Plaintiff, | ) | |
| v. | ) | Civil Action No.: |
| | ) | 2:18cv94 |
| CISCO SYSTEMS, INC., | ) | |
| | ) | |
| Defendant. | ) | |

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia
May 11, 2020

Volume 4
Pages 422-566

BEFORE: THE HONORABLE HENRY C. MORGAN, JR.
United States District Judge

Appearances: (Via Zoomgov Video)

KRAMER LEVIN NAFTALIS & FRANKEL, LLP
By: JAMES RUSSELL HANNAH
Counsel for Plaintiff

DUANE MORRIS, LLP
By: MATTHEW GAUDET
Counsel for Defendant

I N D E X



E X H I B I T S

P R O C E E D I N G S

(Proceedings commenced at 10:03 a.m. as follows:)

COURTROOM DEPUTY CLERK: Civil Action 2:18cv94, Centripetal Networks, Inc. v. Cisco Systems, Inc.

For the plaintiff, Ms. Kobialka, Mr. Noona, are you ready to proceed?

MR. NOONA: We are, Your Honor.

THE COURT: For the defendants, Mr. Jameson, are you ready to proceed?

MR. JAMESON: We are, Your Honor.

THE COURT: All right. Who is going to be the next witness for the plaintiff?

MS. KOBIALKA: Good morning, Your Honor. We would like to first move in some very limited deposition clips that have been provided to you. We swapped out the binder for the new depositions, and there is a much smaller binder for you. I can walk through each of them. The expert will provide an explanation of the testimony that's included in the, in those clips that we are trying to point out for you. So once we've entered those into evidence, then we would, the next witness would be Dr. Michael Mitzenmacher who would be providing an explanation of what all of that means. If you'd like, we could play the clips as well, but we thought since if it's already

moved in to evidence and they're much shorter, that then you, having the technical expert's explanation of what those portions of testimony, how it relates to the technical aspects, would be helpful.

THE COURT: Well, would it be more efficient to just have the expert comment on the clips while they're playing?

MS. KOBIALKA: I mean, we could potentially do that, but I think it helps to frame it so you understand where it comes within the infringement case, having the explanation of where it lies in the various systems. So we will actually call out the specific portions of the deposition clips that the expert's relying upon and then he can help provide any explanation so that would be helpful for you. We could also play the clip and then have him, if you have any questions, he can also provide answers to any questions about that testimony.

The other alternative is we can have Dr. Mitzenmacher testify and then provide the clips afterwards, however counsel for Cisco have indicated they will object on procedural grounds because it was not moved in. That is why we were doing it this way.

MR. JAMESON: Your Honor, Woody Jameson on behalf of Cisco. Our preference, because I think it's about, what, six or seven clips that total about an hour's worth of testimony, is that generally accurate, Ms. Kobialka?

MS. KOBIALKA: Yes.

MR. JAMESON: I think for purposes of understanding expert testimony, having the clips actually played so the record can be developed that way from a, quite frankly an educational perspective, both for the Court and for all concerned, is the way to go. But we do object to the expert taking the stand and testifying about things that are not yet in the record yet.

THE COURT: I think the best way to do it would be to have the expert comment on the clips while they're being played, or just play the part he's going to comment on. If you're presenting technical information that requires an explanation by an expert, I would think the way to present it would be to put your expert on, play that portion of the clip that he's going to testify to and explain while he's on stand, and after he's testified, if there's anything else on the clip that needs to be played, I'll consider it at that time. But I don't see any reason to play the expert -- I mean these clips first and then have him replay them, or portions of them and comment on them. We'd just be going over the same ground twice. So let's just have the expert play that portion of the clip he wants to comment on during his testimony, and presumably that would lay the foundation for any other part of the clip that might be relevant. You may decide that the portion of the clip that he referred to is the only portion you need in your case. So let's proceed in that manner.

MS. KOBIALKA: We'll do so. Thank you, Your Honor.

So at this time my colleague, Mr. Hannah, will be presenting Dr. Mitzenmacher and I will change the name on the screen here. Just bear with me for a moment.

MR. JAMESON: And Mr. Gaudet will be handling the examination of Dr. Mitzenmacher, so we'll be doing the same.

MR. HANNAH: Good morning, Your Honor.

THE COURT: Good morning. How do we spell the witness's name? I guess it'll be on the screen in a moment.

MR. HANNAH: It will, yes. It's Michael Mitzenmacher, and we'd like to call him, and so Dr. Mitzenmacher, if you could put your video on, please?

MICHAEL MITZENMACHER, having been duly sworn, was examined and testified as follows:

MR. HANNAH: Did you want me to spell the name?

THE COURT: No, I've got it off the screen.

MR. HANNAH: Okay. Great. Well, Your Honor, if it may please the Court, may I proceed?

THE COURT: You may.

MR. HANNAH: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. HANNAH:

Q. Good morning, Dr. Mitzenmacher.

A. Good morning.

Q. Let's start out with your educational background. Can you please tell the Court about your educational background?

A. Certainly. I did my under-graduate degree at Harvard University in mathematics and computer science, got my under-graduate degree in 1991. I got to go for a year to the University of Cambridge in England where I got a certificate of advanced study in mathematics, sort of like a master's program there. And then I went to U.C. Berkeley for my Ph.D in computer science, which I received in 1996.

Q. Can you tell us briefly about your employment?

A. Certainly. After I graduated, I went to Digital Systems Research Center. That was a research lab in Palo Alto where I worked from my degree time towards the end of 1996 through 1998. I joined the Harvard faculty in 1999, January 1999. I was promoted to full professor in 2005. I have served a couple of stints as chair, co-chair, the terminology back in 2010 it was called Area Dean, but you can just think of that as department chair. I've also done various consulting work, obviously some legal expert work, but also other consulting work for companies such as Microsoft, Digital Fountain, Eharmony and Akamai.

Q. Can you tell the Court briefly about the organizations that you're a part of?

A. Certainly. So I am a Fellow of the Association of Computing Machinery and a member. The fellows are elected and awarded to the top small fraction of the membership.

I'm also a member and fellow of the IEEE. Electrical and Electronics Engineers, if I'm remembering, or something close to

that. I've served as a couple leadership roles in the Association for Computing Machinery as a member of the editorial board for their main magazine as a chair of what's called the SIGACT, the Special Interest Group on Algorithms and Computation Theory. The Association for Computing Machinery has various sorts of subgroups, and this was one of the major subgroups that I served a leading role for. I commonly serve on, you know, program committees for various networking-related conferences, some of them listed here.

Q. And are you an inventor on any patents?

A. Yes, I am. I am listed, I'm an inventor or co-inventor on the 19issued patents listed here.

Q. And finally, can you tell the Court briefly about some of the awards that you've received in computer networking?

A. Yes. So I've done, you know, first of all I've again been a fellow for the Association of Computing Machinery, and below that you can see the citation. The citation is sort of like what you're listed when you become a fellow, it's what you're known for or what they're making you a fellow for. And it's for contributions to coding theory, hashing algorithms and data structures and networking algorithms.

You know, I've received in the past the IEEE Information Theory Society Best Paper Award for my work on coding theory and networks. I've won the Test of Time Award, again, for some of my work on communications and networks using coding and coding

theory. Early in my career I received the National Science Foundation Career Award. That's an award for, you know, early research stage career academics. Recently, as an example of a recent grant, I have had a grant on privacy preserving distributed storage and computation that covers some aspects of security and privacy. And again, I've done a variety of work on primarily networking, networking communication, and of course aspects of security's related to that.

MR. HANNAH: All right. Your Honor, at this time we'd like to tender Dr. Mitzenmacher as an expert in computer networking and computer security.

THE COURT: All right. Is there any voir dire on that issue, counsel?

MR GAUDET: This is Matt Gaudet for Cisco. No voir dire, Your Honor, and no objection to the tender.

THE COURT: All right.

I noticed we've got a slightly different format today. Instead of having the witness on one screen and the attorney who is questioning the witness, we have four people on the screen, including me. I don't know why.

COURTROOM DEPUTY CLERK: It's your view, Your Honor. Brandan will fix it. It's just your view.

THE COURT: All right.

MR. GAUDET: Your Honor, this is Matt Gaudet. I was going to offer to turn my video off if it made things better,

but if you've got the problem solved --

THE COURT: No, it was just the setup on my screen. I think once we get started then I'll have a full screen of the attorney while he's asking the question and then it'll switch to the witness when he's answering, which is the way we've been doing it. So I think we're fine.

MR. GAUDET: Thank you, Your Honor.

THE COURT: All right. You may proceed.

MR. HANNAH: Thank Your Honor. Is it working properly now with this test?

THE COURT: Yes.

MR. HANNAH: Great. Thank you.

BY MR. HANNAH:

Q. So Dr. Mitzenmacher, can you please tell us, what was your assignment in this case?

A. My assignment was to look at some of the patents under question in this case, particularly the '193, the '806 and the '205, and to examine some of the Cisco products and try and determine whether there was infringement. So the assignment was to look at, in particular, for the various switches and routers with regards to the '193 patent, and similarly for the other patents, and there I was looking also at some of the various management infrastructure that also went in with that equipment.

Q. And here on this slide we have reference to the Catalyst switches, the Integrated Service Routers and Aggregated Service

Routers and the Firepower firewalls. Do you see that?
A. Yes, I do.
Q. And those are the products we'll be talking about today?
A. Yes. Those are the key products.
Q. So if we go to the next slide, can you please briefly remind the Court what are the various patents that you're talking about and kind of our code words that we're using for those patents and what they cover?
A. I'll be talking about three of the patents, the '193 patent, the shorthand is a forward or drop patent. This is going to be talking about various aspects of security policies and setup security policies and how they relate to forwarding or dropping potentially, bad traffic.

The '806 patent has to do with rule swapping and efficiently swapping rule sets when you have the rules change based on new information.

And then the '205 patent is our dynamic security policy patent, and that has to do with, again, issues related to developing or creating a dynamic security policy for certain specific situations.
Q. Thank you. And in forming your opinion in this case what type of material did you rely upon?
A. I've done expert witnessing in other cases, and here, as I have in the past, you rely on the wide breadth of material that you have available, starting of course with the patents and the

file history, obviously the court documents or things such as the claim construction orders or various documents or rulings provided by the Court. And then you start it get into, you know, the various issues related to the products. So then there's understanding the products. I'd look at both public and confidential documents from Cisco. I would look at the product itself or the products themselves in this case, deposition testimony, source code. Again, whatever documentation I could find. And again, hope when I look at these things is to look at all these pieces and try and find the consistency or develop a consistent picture of the products and how they function.

Q. Great. Thank you. And can you please give us a overview or a summary of your opinions before we dive into the dirty details here? What is your conclusion with regard to the '193 patent?

A. For the '193 patent, my opinion was that the accused switches and routers infringe claims 18 and 19 of the '193 patent.

Q. And which products are those that infringe?

A. That would be the Catalyst switches and the Aggregation Services Routers, or sometimes you'll see them as ASRs and Integrated Services Routers, ISRs. I believe the numbers -- and I think we have a slide on this in case I've forgotten any, are the Catalyst switches 9300, 9400, 9500. For the ASR, it's the ASR 1000 series. For the ISR it's also the 1000 series. And

then one of the 4000 series. I think that's the ISR one.

THE COURT: All right. Now there's a slide on that? Because I didn't get all those written down. Do you have a slide with them?

MR. HANNAH: Yes, there's a slide later in the slide deck, Your Honor.

THE WITNESS: I'll have the numbers for you.

THE COURT: All right. Well, let's go through the products again that you claim infringe the '193 patent. Just give them slowly enough that I can make a note of them.

THE WITNESS: Sure. That would be --

MR. HANNAH: So Geoff, if you can jump to Slide 12, please? Thank you.

THE WITNESS: So for the switches, it's the Catalyst 9300, 9400 and 9500 series. These are all part of -- you can see on the left what they're referred to as the Catalyst 9000 platform. And we'll come back to these slides I think, but you can see on the slides various --

THE COURT: All right. I've got that. Let's --

THE WITNESS: Okay.

THE COURT: -- move on to the next product.

THE WITNESS: So this is the ISR and ASR. These are the routers. So see up on the top left, it's the 1000 series for the Aggregation Services Routers. You'll see that referred to as ASRs.

THE COURT: ASR and ISR.

Brandan, can you find me that index of abbreviations?

All right. Next one? Firewalls?

THE WITNESS: Yes. We're looking at various Firepower series and one that's labeled as the ASA with Firepower services. That's on the right you see the Cisco ASA 5500. ASA, let's see, I think refers to -- I forget if it's Advanced Security Architecture or Adaptive Security Architecture. I have my open list of acronyms I can quickly check. But there's the ASA with Firepower and then there's the Multi Firepower series.

THE COURT: That's the 9300 series?

THE WITNESS: Yes. Down on the bottom it's the 9300, the Cisco Firepower 1000, 2100, 4300, 9300, and then the ASA is the Adaptive Security Appliance with Firepower.

MR. HANNAH: Just to be clear, Your Honor, these are for the '806 patent and the '205 patent.

THE COURT: I thought we were talking about the '193 patent.

MR. HANNAH: Right. For the 193 it's just the Catalyst switches and the routers.

THE COURT: Well then, that's all I meant to cover.

MR. HANNAH: Okay.

THE COURT: So these applied to the routers?

MR. HANNAH: Correct. So just so the record's clear, any time we refer to the Catalyst switches or just switches,

we're talking about the Catalyst switches that were just identified, and any time that we refer to the Aggregated Services Routers or the Integration Services Routers or just routers, we're referring to the ASR and the ISR. Those routers.

THE COURT: Well, how are you going to approach this? Are you going to go through the switches and then move to the routers? Is that the way you're going to do it?

MR. HANNAH: Well, Your Honor, for the '193 patent it's actually a little bit easier in that it's the same operating system, so it's the same software on both and so we'll just --

THE COURT: On both of what, the '205 and the '193?

MR. HANNAH: No. For the proofs for the '193 patent, we're going to be able to run through the switches and the routers at the same time because they have the same software on them. So we'll be doing them together.

THE COURT: All right. It's up to you how you want to do it.

MR. HANNAH: Okay. And just to --

THE COURT: See, this has the '806 patent up there.

MR. HANNAH: Right. So he's an expert and provides his opinion on three of the patents.

THE COURT: I understand he's doing '806, but I thought we were on '193 at this point. We're not?

MR. HANNAH: Yeah, we can -- we'll start with the '193

and just go through that and then we'll do a transition to the '806.

THE COURT: I think that would make it more understandable.

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. So Doctor, before we get into the '193 patent I do want to show you a demonstrative that we created over the weekend to show the Court, which is the OSI model, the Open System Interconnection model. And Dr. Mitzenmacher, you remember the Court had some questions regarding the different layers that we were talking about. We had Layers 2 and Layers 3. Do you remember that from the Court?

A. Yes.

Q. Can you just briefly inform the Court as best as you can the different layers that we're talking about and how they're going to be relevant to your testimony today?

A. Certainly. So in networking, they have developed -- there are actually a couple of these, the most standard is the -- or one of the standards is presented here, it's called the Open System Interconnection, or OSI model. And here, I do want to emphasize that this is really just a model. It's a way of helping to think about different aspects of what goes on with networking. It is a model, and depending on the situation, may or may not closely correspond to the reality. But the idea is

that you can think of what's going on as various layers, where the upper-level layer will call upon the lower-level layers.

So at the lowest level, we talk about the physical layer. So you can think of this as like this is where the wire is, or where the actual, you know, information, the bits, the signals, are being transferred.

So up above that at the next level is the level of like the individual data links. And you can think of this as the layers where generally the switching that we've been talked about occurs. So you can think of it as being, generally speaking, you know, within a network or a subnetwork, and that this is sort of the direct communication from sort of one machine to another, again, possibly through a switching device which will make that sort of connection.

And up above that is the networking layer which deals with communication between different, potentially between different networks based on -- and sets up an address framework so that you can label machines on a network or in various networks based on the, what's called the Internet protocol or the Internet protocol address.

And there are further layers up on top which handle other aspects of communication. Something which may come up is what's sometimes called Layer 7 or the application layer. You can think of this as sort of the top layer. This is up, in some sense, above the network and talks about the applications that

may be using the network for communication such as, you know, Microsoft Office or Skype or any of the upper-level applications that -- email, that may require communication services.

One of the things that come up is in these layers, you can have various sorts of header information which provide things like address information, where is this object, this packet supposed to go to. And sometimes you hear of things like payload which often corresponds to, say, application-level data. So you know, these can be various parts of a packet. We may be talking about header information particularly in the context of Layers 2 and 3. That is sort of the actual networking, switching, router communication layer. And sometimes there may be discussion of data in the form of payload data in particular which corresponds to Layer 7 information.

THE COURT: All right. Okay.

BY MR. HANNAH:

Q. Thank you, Doctor.

Let's turn to the Catalyst switches that we'll be talking about first for the 193 patent. And Doctor, at this time I'd like to show you PTX-1260.

Doctor, do you recognize PTX-126?

A. Yes. PTX-1260 you can see up in the right. It's labeled White Paper Cisco Public. This would be information that Cisco would make available to its customers in order to describe or advertise this family.

THE COURT: Let me get the exhibit book here.

We're looking at 1260?

MR. HANNAH: Yes, Your Honor.

THE COURT: All right. I'm sorry, can you start with 1260 again from the beginning?

MR. HANNAH: Sure.

BY MR. HANNAH:

Q. Go ahead, Doctor. Can you just explain what PTX-1260 is?

A. Sure. If you look at the top right corner you can see the very small font, but it says White Paper Cisco Public. This would be sort of a typical document Cisco might give to its potential customers or customers to describe this family of products.

Q. If you look at the bottom left-hand corner there's a copyright date of 2018. Do you see that?

A. Yes, I do.

MR. HANNAH: All right. Your Honor, at this time we'd like to move PTX-1260 into the record please, into evidence.

THE COURT: That will be admitted.

(Exhibit PTX-1260 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

Doctor, if we can go to Page 7 of this document?

And, Your Honor, it should be the very next page in your binder.

BY MR. HANNAH:

Q. Page 7 of this document, can you explain what's being shown here in terms of describing the Catalyst switches?

A. Right. So this is showing a key aspect that we'll be discussing throughout my testimony with regard to this switch, set of switches, is that these switches were developed, as it says, to be a critical part of an end-to-end integrated security solution. So these products were designed with security in mind, and in particularly, as I'll be showing, there are multiple situations where the switches themselves are part of an effort to detect and stop threats, as it says in the next line. You know, it can get information from other aspects of Cisco or from various threat indicators. You know, there is some discussion of, for instance -- well, we'll discuss the various Talos and other systems as we go forward.

Then I think if we look at the bottom --

THE COURT: Well, this product has the ability to detect and divert or drop; is that correct?

THE WITNESS: Those are two of the, some of the features it has. It plays a role or can provide information for other aspects that the DNA Center -- that's the Digital Network Architecture Center we'll be talking about detection. In particular for this patent, the '193 patent, I'll be focused on the issue of stopping threats or dropping as dropping or sometimes it's called blocking as it relates to the patent.

THE COURT: Well, seems to me we had some evidence of

some products of Cisco's that only detected threats or malware and didn't act on the threats. Does this product have the ability to act on the threats it detects?

THE WITNESS: Yes, very much. So what will happen, as I'll discuss, is that it is given information or given policies based on the detected threats from the DNA Center, from the Digital Network Architecture Center through also such components of that architecture, as you can see below on the bottom, it talks about infringes the ISE, the Integrated -- sorry, the Identity Services Engine. And I'll be talking about how those relate to each other and in particular why it is that that means that this product does drop or block traffic based on rules and policies. That's going to be something I'll be spending a lot of today talking about.

BY MR. HANNAH:

Q. And Doctor, in this trial so far we've heard testimony about inline and out-of-band. Does the Catalyst switches, do they block threats inline?

A. Yes, they do. That's one of the terminologies I guess you could use to describe it. You know, the switches are receiving packets as they come through the network, as they travel through the network, and the switches will block them, drop them, keep them from reaching their destination, and so that the traffic can't reach the end host or be sent out from the end host in some circumstances as well.

Q. All right. So for the '193 patent, we'll actually be talking about the routers. This is the Aggregated Services Router and the Integrated Services Router.

MR. HANNAH: We'll just, Your Honor, if it's all right, we'll just call those the routers for shorthand, because they operate in a similar manner for infringement purposes.

THE COURT: All right. We've been talking about switches, now we're switching over to routers, right?

MR. HANNAH: Yes, Your Honor.

THE COURT: Okay.

BY MR. HANNAH:

Q. So if we could just introduce, let's just introduce the routers, Doctor. And if we can go to PTX-1226?

THE COURT: I've got it.

MR. HANNAH: Thank you.

BY MR. HANNAH:

Q. Doctor, can you please explain for the Court what is PTX-1226?

A. This again would be another high-level document describing the routers and router solutions. If you look up in the top left corner, you can see it says, again, At A Glance Cisco Public. So this would be the public information that would be used to describe the products, for instance, I imagine, to potential customers or current customers.

Q. Doctor, looking at the first couple paragraphs, do the

Cisco routers, do they have the ability to stop threats and provide security?

A. Yes, they do. I mean, it's described here as integrated security. Part of that integrated security with regard to routers is, again, the ability to block or drop traffic as needed. Again, the routers are a main inline device which will be used to determine whether or not traffic is allowed to continue, whether it's forwarded, permitted, or instead, whether, based on the security rules and policies, it needs to be dropped or blocked.

THE COURT: Let me ask a basic question here. The difference between a switch and a router is that the switch simply allows the traffic to enter or keep moving in the network, but the router is used to send it to a particular destination? It might be an intermediate destination, but it sends it to a particular destination, is that accurate?

THE WITNESS: So at a high level, yes, that's accurate. So switches are typically used internal to a network. So once it's inside, say -- I think they have used the analogy of your courthouse, and routers could be used to send to other places, in particular to other networks. And as you've pointed out, routers, it may not be an immediate jump, it may be that the routers themselves cause it to go to other intermediate locations along the way; that is, it passes through a series of routers until it reaches its final destination.

THE COURT: All right.

THE WITNESS: These days, Your Honor, even internal networks are, can be quite complicated and can be set up with various internal subnetworks. You know, I think there's been discussion of things like, well, you know, this part of your organization may have higher security or higher levels of, more secure protocols than other parts of your network as to who can get in. And so switches themselves contain some of this similar functionality to routers, but generally are kept within an internal network and its corresponding subnetworks. So you may also find, just as you said, like switches may have to go through intermediaries or so on. You'll see the same thing inside a large organization's network as well using switches.

THE COURT: All right.

BY MR. HANNAH:

Q. That leads us to the next topic here, which is the operating system of the switches and routers. Doctor, do the switches and routers share the same rating system for purposes of your analysis?

A. Yes. By the way, sorry if this already was -- was that already admitted or does this need to be admitted as evidence?

MR. HANNAH: Oh. Thanks, Doctor.

Your Honor, I'd like to move in PTX-1226 into the record.

THE COURT: 1226 will be admitted.

(Exhibit PTX-1226 received in evidence.)

THE WITNESS: Sorry about that.

MR. HANNAH: I appreciate it.

THE COURT: All right. Operating systems.

MR. HANNAH: Right.

THE COURT: Does that lend itself to a definition? Operating systems?

THE WITNESS: Well, so the operating system --

THE COURT: Is that the source code? Is that what we're talking about? Source code?

THE WITNESS: Yeah. I mean, it's possible that you can imagine parts of the operating system embedded in hardware. But typically it would be the source code, and it's the code that runs the hardware or it's the code that runs the system. So for instance, I'm not sure what type of computer you're using, but if it's a like a Microsoft Windows PC-based computer, right, that, you know, Windows or its current offshoots or variants would be like the operating system. So without an operating system, your computer is typically a lump of hardware, but it can't necessarily actually do anything because it needs something giving it sort of the baseline instructions of what it can do and how it's going to interact with the hardware. And that's really the operating system. Like you said, it's code, it's code that interfaces with the hardware, and essentially any instructions that you're trying to give to the hardware, like

with an application program, your Microsoft Word or your Zoom, is going to use or run through the operating system to tell the hardware specifically what to do.

THE COURT: All right.

BY MR. HANNAH:

Q. So Doctor, I'd like to show you PTX-242.

Looking at this document, can you explain what's the name of the operating systems for the routers and the switches that we'll be talking about and what this document shows?

A. All right. So --

THE COURT: Just a moment, please.

THE WITNESS: Certainly.

THE COURT: All right. I have PTX -- we were on 1200. We're going backwards now. 242.

MR. HANNAH: 242, yes, Your Honor.

THE COURT: Okay. PTX-242. All right. You may proceed.

MR. HANNAH: Thank Your Honor.

A. This is a document again from Cisco describing at a high level their operating system. So for these devices, you know, Cisco has developed its own operating system, not unsurprisingly for -- or unsurprisingly, sorry, for its devices. So it refers to it as the Cisco iOS, or in particular, the Cisco iOS XE. And there are different versions that come out. This is a high-level description of, you know, the Cisco iOS XE 16

version.

THE COURT: What does the "i" stand for?

THE WITNESS: I feel like I want to say Integrated.

THE COURT: Well, let me look at that. Well, they have got IOS XE. Internetwork Operating System XE. I guess XE is just the title of it, according to my list of abbreviations.

THE WITNESS: All right. We'll go with yours.

THE COURT: All right. You may proceed.

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. So Doctor, if we went to PTX-242 and if we go to Page 4 of this document, can you show us what operating system is on the Catalyst series switches?

A. Right. So you can see I guess now up at the top where it says Enterprise Switches, that's the 9300, 9400, 9500 which we previously listed as the various infringing products, make use of the Cisco iOS XE. That's the operating system.

Q. And then if we look at the routers, the various routers, can you identify for the Court the operating system of the various routers?

A. Here it's the ISRs, and if you'll recall when we talked about the ISRs, we said they covered the 1000 series and the 4000 series. Then you can see the 4000 series has various sub-numbers.

THE COURT: Wait a minute.

THE WITNESS: Oh, sorry.

THE COURT: Okay. we're looking at a different document here?

THE WITNESS: No. Same document, it's just the next page.

MR. HANNAH: Pages 4 and 5, Your Honor.

THE COURT: All right. So these are called branch routers?

THE WITNESS: That's how they're referring to them here. That would be, I suppose, meant for a branch of the organization, like a large office.

THE COURT: Are you saying that all of these infringe?

THE WITNESS: Yes. I believe this is the 1000 and 4000 series. All of these are in the 4000 series.

THE COURT: And these have the same operating system as the switches we just talked about; is that right?

THE WITNESS: Yes, they are all actually running the same operating system.

THE COURT: And it's the operating system that infringes, is what you're saying?

THE WITNESS: Well, I'm saying that the products themselves are what infringes, but certainly a big part of the argument -- or for instance one of the reasons I'm going to discuss them all together for many of my arguments is because they use the same operating systems. So they have the same code

and instructions. And as you point out or when we look at the claims, like the claims are system claims or computer-readable media claims, and the CRM claims, yes, are based on the software that's being run, and in particular the operating system.

THE COURT: Okay.

BY MR. HANNAH:

Q. If we go above that we have the list of the ASR products. Are these the ASR products that infringe in your opinion, Doctor?

A. Yes. In particular I think we've said the ASR 1000 series. So it would be all the ones that are 1000 and something.

THE COURT: All right. Let me make a note of that.

MR. HANNAH: Your Honor, at this time I'd like to move PTX-242 into evidence.

MR. GAUDET: No objection.

THE COURT: That will be admitted.

(Exhibit PTX-242 received in evidence.)

MR. HANNAH: And for convenience, Your Honor, just to identify for the record, the list of products is on Bates number 478816 and 478817.

THE COURT: 478816 and 17. All right.

BY MR. HANNAH:

Q. All right. Doctor, I'd like to turn our attention now to the Digital Network Architecture that's been referred to as DNA, but we'll try to avoid the acronyms as much as possible. Can

you explain for the Court what is the Digital Network Architecture?

A. Yes. So the Digital Network Architecture, so one of the issues I think that's come up a lot in our discussion, right, is that these issues of there are these devices like the switches and routers that we're talking about right now that get these rules that determine what traffic is allowed to pass and what traffic isn't allowed to pass. And a question comes in, like, well, you know, where do they get these rules? You know, how are these rules decided? And the Digital Network Architecture is the management structure that allows it to take in or utilize these sort of threat intelligence, operationalize it, and turn it into rules and policies that these switches and routers use to determine what is safe and what isn't safe. The Digital Network Architecture includes the, what's called the DNA Center, that's sort of the device which, you know, sends out or promulgates these sets of rules. It also in some sense I would say absorbs the various threat intelligence and uses that to determine rules and send them out.

And I should say that when I'm talking about the Digital Network Architecture, I may focus a lot on the DNA Center, but it includes -- the architecture includes other additional components that you have heard about, things like StealthWatch and the Identity Services Engine as well.

THE COURT: Well, what would you call StealthWatch?

Is that an operating system? What is it?

THE WITNESS: So StealthWatch, I think I would probably refer to it as a component of the Digital Network Architecture. It would include its own operating system. StealthWatch is part of the architecture that gets served telemetry information, so it gets measurement information as well as threat intelligence information of various types, and as part of this Digital Network Architecture, part of this whole group, provides or gathers, absorbs threat intelligence information to get passed out and circled into the system with new rules, new policies to prevent security threats.

THE COURT: Well, when somebody says StealthWatch infringes the patent, I mean, StealthWatch is part of the DNA?

THE WITNESS: Yes.

THE COURT: All right. Well, StealthWatch is to DNA as the operating system is to the switches; is that right?

THE WITNESS: I can see the analogy you're trying to make. It's certainly, you know, the StealthWatch is gathering and providing information that gets used in determining these new rules. I'm a bit hesitant on the analogy because, again, the operating system is really something sort of specific that you layer on top of a device to allow additional software to interact with the hardware. And the StealthWatch, you know, has some aspects of that, it's certainly getting information from the various other sources, so you can say that there's other

things running on top of it, but it's sort of at a different level. It's a bit higher of a level. A bit more application-oriented. StealthWatch itself for instance would have its own operating system underneath it.

THE COURT: Well, would StealthWatch --

THE WITNESS: I can see your analogy.

THE COURT: Would StealthWatch fit into the levels we talked about? Would it come in in one of those levels?

THE WITNESS: Not really, because that's sort of talking about the network infrastructure and how packets move around whereas, again, StealthWatch is itself you could think of it's referring to a hardware device with various applications running on it.

THE COURT: Okay.

BY MR. HANNAH:

Q. Maybe we can jump ahead here to PTX-1281, Doctor and we can -- you can describe how StealthWatch is integrated into the DNA Center. So if --

A. Okay.

Q. -- we blow up where it says "The integration with StealthWatch security provides detection and mitigation of threats."

A. Certainly. Let's see. Right. I can try and underline it on the screen or may be Geoff if you can underline it -- yeah, it's integration --

THE COURT: I see where you are. Yes.

A. Okay. So the "Integrated with Cisco StealthWatch Security provides detection and mitigation of threats even when they're hidden in encrypted traffic." So the StealthWatch device is going to look at various sorts of information, measurement information, telemetry information, determine what's going on, as part of that, it, in conjunction with the other aspects of the Digital Network Architecture, will try and determine if there's something odd or worrisome or a potential security threat that's going on, and use that to come up with, you know, new rules or new actions, and feed that back into the switches and routers, which is for the '193, what I'm going to be focused on, it actually what's going on at those switches and routers. But something has to give the switches and routers their marching orders. Something has to give them the rules and the policies which says this is okay, this is not okay, right? And so StealthWatch is part of that. StealthWatch is part of that system which is determining, which is saying, hey, this is a problem, this is what you as the switches and routers need to do about it.

THE COURT: Well, some examples of what StealthWatch might look at would be the header, the volume --

THE WITNESS: The volume of that information, for instance. And I'll actually be talking about that with the '193 patent, because the '193 patent will be talking about what's

called exfiltration. So that's when we'll be looking at things like when data is being taken out of your network, and one of the signs of that is if you see an unusual amount of volume, if you see lots of data looking like it's leaving your network and you don't know why, that might cause your system to say, wait, I'm not going to allow this information to leave until I get a better handle of what's going on.

THE COURT: Well, can StealthWatch look at -- well, if it's encrypted they can't look at the content, they can only look at the source or the volume or the recipient or --

THE WITNESS: Exactly. So one of the things StealthWatch can look at are things like, even if it can't look at the content, it can determine the volume and where it's going and where it's going to and from, which would be the sort of information you might use to determine if there's an exfiltration attack.

BY MR. HANNAH:

Q. If we can go to PTX-992 just to kind of help us? If we go to the second page, I believe, and it talks about the Predictive Threat Analytics, and specifically the Cisco Talos Threat Intelligence. Does StealthWatch also use what Dr. Moore talked about as CTI, or threat intelligence, in order to make blocking decisions?

THE COURT: Do you want 1281 admitted?

MR. HANNAH: Yes, Your Honor.

THE WITNESS: I was going to remind him too, Judge.

THE COURT: All right.

(Exhibit PTX-1281 received in evidence.)

THE COURT: 992 we're looking at now.

MR. HANNAH: Your Honor, we'd also like to move PTX-992 into evidence.

THE COURT: All right.

(Exhibit PTX-992 received in evidence.)

BY MR. HANNAH:

Q. If you could show both this predictive threat analytics paragraph and the next paragraph, I think this will help with the examination in terms of what is the type of information that the DNA Center using StealthWatch can operate on.

A. All right. So StealthWatch, and again, the entire Digital Network Architecture including the DNA Center is working on, is a variety of information. So part of it is, as it says up at the top, it's looking at your own network and looking to see if there's any unusual behavior, and using statistical techniques that referred to as machine learning to determine if there is various sorts of threats going on in your network. But it's also combining this with various sort of threat intelligence. It says here that the Cisco Talos Threat Intelligence. So these are, you know, not just what it sees on the network, but it's combining this with the threat intelligence from other additional sources. So it's essentially trying to get together

all the information it can and use that to help determine what are the rules, what are the policies down at the actual device level of the routers and switches. As new threats or problems appear, you're going to need to go back to these routers and switches and say, okay, something's up, you need to change the behavior, you need to block this connection or drop this type of packet, and that sort of feedback is what allows for the switches and routers to play an active role in the security of the system.

THE COURT: So this is detecting threats after they have entered the network?

THE WITNESS: So I would hesitate --

THE COURT: Do we have -- I mean, does StealthWatch work at the gateway to the network?

THE WITNESS: Well, StealthWatch -- so the way to think of it is, again, StealthWatch is gathering information and it's gathering information from a variety of sources, okay? So part of that it's monitoring what's going on in your network, and it can see suspicious activity that's going on in your network. And again, the goal is to actually prevent the damage, right? So ideally it can do that, it will actually stop the damage before it still actually occurs.

Now, that's part of the network monitoring, but again it's also getting threat intelligence. It's also getting information from other sources. So it can also help in

preventing attacks, as I think you've phrased it, before they happen, right? There's not such a fine line in the sense that some of it is based on things going on in your network, and there it's both trying to stop things that may be going on or have just started as well as things that have already entered your network, but it's also trying to prevent things from getting into your network to begin with. And it does that also by means of things like threat intelligence.

THE COURT: Well, is there anything about the patents themselves or StealthWatch which makes it easier to detect threats after they have entered a network than it would to detect them at the gateway to the network, or does that make any difference?

THE WITNESS: So I think we're getting into details that might be better when we get into the discussion of the specific patents, because the different patents have sort of different goals and criteria.

I would say with the exfiltration, for instance, that there's not such a fine line. Because your goal is to notice things and stop the exfiltration before it actually happens. It may also be useful to notice the exfiltration and then say, a-ha, this did happen, and then you have to take remediation efforts. But I'd say one of the big goals is to actually stop it before it actually takes place on any large scale. So notice it at the beginning and say let's shut this down and stop it

before it actually takes effect and becomes the threat.

THE COURT: All right. If I ask you a question that's jumping ahead of something, you can just tell me --

THE WITNESS: Okay.

THE COURT: -- we'll cover that subsequently.

THE WITNESS: Okay. I think you're asking good questions, and I think we'll get more information about them as we're going forward.

THE COURT: All right.

A. Maybe just looking at the second paragraph, again, it's going to give you an idea, you know, it's talking about detecting threats like unknown or encrypted malware, insider threats, you know, insider threats, exfiltration is certainly an example of those. And you know, as it says in the last line, "It integrates with your existing security controls to respond to the threat without any business shutdown." And I'll be describing I think more specifically how that works.

THE COURT: Well, but you qualify -- I just finished saying Friday I guess that it's difficult to define artificial intelligence, but is the ability to detect the potential threats before they cause damage, is that --

THE WITNESS: That is definitely one.

THE COURT: -- artificial intelligence? The fact that it's learning as it goes along, sort of, would meet your definition of artificial intelligence?

THE WITNESS: Oh, I think, I think artificial intelligence is very broad, and so I would be careful of trying to limit it too much. But certainly in this context what the artificial intelligence, like you said, is doing, is seeing a particular pattern or noting something out of place and trying to stop it, like you said, before damage occurs.

BY MR. HANNAH:

Q. And Doctor, if you look at what's being shown on screen as this, shown with the supervised and unsupervised machine learning?

A. Yes. So that's the way it phrases it here. It says it can pinpoint anomalies which are further analyzed using a combination of supervised and unsupervised machine learning from high-fidelity threat detection. So it's looking for patterns, seeing something that's not right, studying it and trying to stop it before actual damage occurs.

THE COURT: All right.

BY MR. HANNAH:

Q. So let's turn to your infringement opinion, Doctor. Now, are the switches, the routers and the firewalls, are they made and used in the United States?

A. Yes.

Q. And how do you know that?

A. I know that from various sources. In particular I think to start was Cisco's responses for information.

Q. So I'd like to show that to you. It's PTX-1409.

MR. HANNAH: And these are Cisco's objections and responses to our Requests for Admission.

THE COURT: I've got it.

BY MR. HANNAH:

Q. Doctor, did you rely upon these responses to Centripetal's Requests for Admission in forming your opinion?

A. Yes.

MR. HANNAH: Your Honor, I'd like to move PTX-1409 into evidence.

MR. GAUDET: Your Honor, the objection -- we don't have any problem with them relying on anything that we admitted, but moving an entire discovery response with objections and various requests and things that were admitted or denied or partially admitted just seems a bit over-broad. We certainly do not have a problem with Dr. Mitzenmacher relying on anything that we admitted though.

MR. HANNAH: Your Honor, we will only, we only need to admit Pages 5 and 6 into the record.

THE COURT: Well, that's --

MR. HANNAH: We can also read it into the record, Your Honor.

THE COURT: Well, I think we can admit this -- I think the Court can separate the wheat from the chaff.

MR. GAUDET: Thank you, Your Honor.

(Exhibit PTX-1409 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. So if we can go to Page 5 of this document, and if we look at the Response to Admission No. 1, Doctor, can you tell the Court how this informed your opinion as to whether the source code for the accused routers, which is the -- well, this is the second one, so let's start with the first one. With the accused firewalls which is referred to as the ASA products here, how does that inform your opinion?

A. So the Admission No. 1, since you're referring to that, the firewall products, and it simply says "Cisco admits that it compiles the source code for the accused ASA products and services in the United States."

Q. And what does that mean, "to compile source code"?

A. Right. So I wish I had a demonstrative. Should have thought of that. Compiling is -- so source code is written by engineers, by coders in the company, and written in a high-level language that humans can understand. So it's really important that humans be able to write code that, both for their own understanding, but so they can look at it and read it and understand it later, and we'll be seeing some source code I think later in the course of my testimony. So again, source code is written at the high-level human level. The computer instructions are in what are sometimes called machine code or

object code. It's at a lower level. And it's really generally impossible for a human to read or understand. It's meant for design for the computer. So the computer instructions can also be very low-level, like add this number to this number or turn this bit on or off. So there are tools called compilers, and what they do is compile the code. They take the source code and they translate it or turn it into the machine code that gets used by the actual hardware. So when it says compiles the source code, that is in some sense taking the large, high-level source code that humans have developed and turning it into the actual instructions that the machine will run to be put on the machine.

Q. Is it fair to say, when someone admits that the source code is compiled, that they're making and using the product? Is that fair?

A. Yeah. That's part of, certainly part of making the product, and then once the code is compiled then you would use it.

Q. If we go to Request for Admission No. 2, the response to that, do you see where its says "Cisco admits that it compiles the source code for the accused router products and services as Cisco has defined that term in the United States?" Do you see that?

A. Yes.

Q. Is it your understanding that the accused routers, router

products and services are the ASR and the ISR products that we described earlier and will be talking about today?

A. Yes. I believe that's -- yes, that's what we've discussed.

Q. If we go to Request For Admission No. 3 and look at the response to that, Cisco -- just reading the document -- it, says "Cisco admits that it compiles source code for the accused Catalyst products and services as Cisco has defined that term in the United States." Do you see that, Doctor?

A. Yes, I do.

Q. And how does that inform your opinion with regard to the accused Catalyst products and services?

A. Similarly, the make or use terminology, that shows that they make the product or make the corresponding product, in particular the compiled code, in the United States.

Q. And when it's referring to the accused Catalyst products and services, is it your understanding that that's the Catalyst switches that we've been talking about and will be talking about today?

A. Yes.

Q. With that, let's turn to the '193 patent. I'd like to bring up JTX-4.

MR. HANNAH: Has already been admitted, Your Honor. This is the '193 patent.

THE COURT: All right. I think this should be a good time to take our morning recess.

MR. HANNAH: Good. Thank you, Your Honor.

THE COURT: We'll be in recess until 11:45.

(Recess taken from 11:25 a.m. to 11:45 a.m.)

THE COURT: All right. You may proceed. Thank you very much, Your Honor. May it please the Court.

BY MR. HANNAH:

Q. Doctor, I'd like to show you JTX-4. This is the '193 patent. Do you recognize this document, Doctor?

A. Yes, I do.

Q. And what is this document?

A. Well, it's a front cover page of the '193 patent that we'll be discussing, that I've studied.

Q. If we go to the next slide, what claims are we going to be talking about today?

A. 18 and 19.

Q. And can you just briefly remind the Court what does the '193 patent cover?

A. We talked about this as the Forward or Drop Patent. So we'll be discussing it in the context of forwarding or dropping, and I'll be discussing the specific scenario, but related to exfiltration.

Q. Before we get into that, just want to show you the claim construction that's been entered into this case.

Doctor, in providing your opinions, did you apply the Court's -- the agreed parties' claim construction in forming

your opinion?

A. Yes, I applied the agreed constructions in forming my opinions.

Q. Did you also apply the Court's claim construction in forming your opinions?

A. Yes, I applied the Court's claim constructions in deriving my opinions.

Q. Thank you.

So if we turn to the next slide, can you inform the Court what's being shown here on this demonstrative?

A. All right. So this is a demonstrative sort of showing what's going. What's going on at a high level on the claims will be, you know, more complicated. But what's going on at both the routers and switches is there are various rules which determine whether a given packet, which again is represented by the box, is allowed to continue or not to continue based on certain rules. And in particular, there are rules that these switches and routers use that are, they receive in order to prevent or stop certain types of attacks which relate to the claims and the claim element.

Q. And the slide says "Forward it or drop." Does that also mean block?

A. Yeah. I'll try and use the claim language where I can. Sometimes you'll hear forward or drop, sometimes instead of forward you'll hear permit, or sometimes instead of drop you'll

hear block.

Q. And the packet is -- what you're representing the packets are traveling along this conveyor belt. Does the traffic go -- do the switches and routers, do they inspect traffic in both directions?

A. Yeah. I mean, they inspect traffic that might be coming to an endpoint or might be going out from an endpoint. So it might be coming from your computer or going to your computer, and the switches and routers would examine the traffic going both ways.

Q. Go to the next slide, we heard, I guess last week, Dr. Moore talking about exfiltration and how the '193 protected against exfiltration. He explained to the Court what data exfiltration is and how the '193 patent applies to that.

A. Sure. So data exfiltration is a particular type of attack where you're trying to pull data out of the secure network. So for instance, I recall discussion of things like credit card numbers, right? So if you're protecting credit card numbers, you don't want that credit card, those credit card numbers leaving your internal network and getting out into the outside world, because that creates headaches and problems for everyone. But you know, for any corporation, they may have some confidential or private information where they have information that they don't want leaking out of their internal network out into the outside world.

Now of course sometimes some of that information may be

useful to let out to a corporate partner or to some other location where it's perfectly fine to let that information out, or it may even be that it's like, well, I have some financial information in my finance department, and I generally don't want the finance information getting out, but if it goes to the subnetwork or the CEO or the other high-ranking officers, that might be okay.

So what this slide is showing -- and this works for both the switches and routers -- is that you can have packets that there's places from your internal network that it may be okay to reach, either okay to send or to get information from, and there may be applications that it's not okay to reach, and in that case, you know, packets should be denied. And the idea here is you might prevent exfiltration by preventing people from getting too much data from some internal place in the network, or you might prevent it by potentially not letting them push information out of the network, depending on the situation.

Q. And so does this type of technology, does it protect against threats after the fact, after a computer has already been infected?

A. So this type of, I would say, is designed, when you're looking at exfiltration attacks you're really just trying to do both, right? So it may be that it's something that takes enough time that you don't notice until after the fact, but ideally, particularly if someone is gathering a large amount of

information that they're not supposed to be gathering, and you notice that quickly enough, you can develop a rule that blocks them from either gathering more information or potentially transmitting that information out, depending on how quickly you gather that information.

For exfiltration attacks, usually those are usually sort of slower sorts of attacks because -- or often they can be slower sorts of attacks because it may take time to either find or gather the information you're looking for.

Q. And I believe you testified to this, but the exfiltration techniques that we'll be discussing, this applies equally to both the Catalyst and -- the Catalyst switches and the ASR and ISR routers?

A. Yes. It applies to both of these devices.

Q. All right. So I'd like to show you PTX-995.

THE COURT: I've got it.

MR. HANNAH: Thank you.

BY MR. HANNAH:

Q. Doctor, can you explain, what is that document?

A. It's titled Cisco Security Analytics. Again, if you see up in the upper left-hand corner, it's a white paper, Cisco Public. So this would be, you know, information Cisco would be providing to customers or potential customers generally.

MR. HANNAH: Your Honor, at this time we'd like to move PTX-995 into evidence?

MR. GAUDET: No objection, Your Honor.

THE COURT: That will be admitted.

(Exhibit PTX-995 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. Doctor, I'd like to turn to Page 8 of this document. In particular, look at the paragraph that says Insider Threats. Can you explain what's being shown here in this document and how this relates to exfiltration technology of Cisco?

A. Right. So that's talking about these certain insider threats where they're talking about the data breaches, right, data breaches cost organizations millions of dollars, right. So again if we're talking about someone coming in and stealing your credit card information that's getting the credit card information from a company, that's an obvious threat. Maybe less obvious is, again, internal employees who end up gathering information and providing it to a competitor. So it talks here about hoarding data, disgruntled employees, hoarding data in order to export it to the outside for financial gain or just to cause harm. So these sorts of behaviors might be looked at or determined by the Cisco devices like StealthWatch, but then what we are interested in this patent is sort of the result. You know, once you've determined the potential threat, you need to stop the event from happening if you can. Or certainly stop any further action. And so if you look at the bottom, it talks

about quarantining. So StealthWatch can quarantine the suspected host off the network. And this is enabled by the integration with the Cisco Identity Services Engine. That's the ISE that we've talked about before. And so I'll be talking about sort of the methodology that, the quarantine method that it uses. But at a high level, the idea is that the natural thing -- if you start to notice, for instance, that an employee is gathering data from a location that they don't normally gather data from, and that data is sensitive you might say, okay, I'm going institute a rule to shut down or stop this employee from either accessing this information, might be one possibility, or you might stop them from going out to the Internet, depending on what sort of security action you think is appropriate.

Q. And so when we were showing the skull and crossbones on the previous slide, was that showing that the laptop was being quarantined from the network by the switches and the routers?

A. I believe so. That's a common symbol. And we'll be looking again at more detail about what is actually, how the quarantine takes effect.

Q. Right. Let's take a look at the claims.

So we have on the slide portions of claim 18 and 19. You have them side by side. Can you explain why you put them side by side in terms of your analysis?

A. So the two claims, one is a system comprising, and then

there's some other, you know, preambulary or first, a system comprising, then sort of the first elements describing that it have a processor and memory and so on. And then for 19, it's a computer-readable medium claim. So it's talking about comprising instructions that, when executed, cause the computing devices to do the following. So beyond that, the steps are, as I recall, are identical.

So one is a systems claim, and one is a computer-readable media claim, as we talked about before. That relates to the operating system and the instructions and sort of the software that makes these devices run for the computer-readable medium claim. But I'll be treating the two claims together because really they are the same except for this aspect that one's a system claim and one's a computer-readable medium claim.

Q. Is it fair to say that claim 18 is directed to the system and then claim 19 is directed to the software on the system?

A. Yes.

Q. And other than the first elements we have in the bottom, all of the other elements are the same, so we'll be treating these together for our analysis today?

A. Yes.

Q. And also because the Catalyst switches and the routers share the same software, can we group those as we do our proofs today?

A. Yes. As we've discussed, they run the same operating

systems.

Q. If we go to the next slide?

What is computer-readable media specifically?

A. Computer-readable media could be like software that you actually load into your computer through something like a CD-ROM or a memory card, or it might be something that's installed on your computer, you know, through a hard drive or a USB drive. It may also be programmed in inside aspects of the hardware. You know, that includes things like the hard drive and so on. So there are a variety of media that can be used to store instructions for your hardware, and I don't think it's limited to any specific computer-readable media type.

Q. What are the instructions that are on the computer-readable media?

A. So again, that would be, like we've talked about before, generally that would refer to things like the compiled code. So the operating system gets compiled, it gets turned into machine-level instructions. The idea here it's showing it as a bunch of zeros and ones. These instructions, when you're looking at them at the computer level, you know, humans would have -- even experienced humans would have a grave difficulty to impossible reading them. But they're stored in a way that the computer understands them on a hard drive or some other media.

Q. All right. So if we turn back to the claims --

THE COURT: Well, how do you get the program, the

operating program onto the hard drive?

THE WITNESS: So typically that would --

THE COURT: The hard drive can just read it and retain it; is that right?

THE WITNESS: Yes. That would be loaded in -- like before your box is shipped to you, the company would put the operating system on. Alternatively, for some types of hardware, it may be that you get it and there's some sort of minimal device functionality so it can connect to the Internet, then it would download the operating system. Depending on the device, that could take a long time. And then it would be stored on the hard drive, say. There are a variety of ways to get it on the hard drive. Typically it would be pre-installed or, you know, when you have an update, for instance, you would download it and then it would be stored in the hard drive or whatever media you're using.

THE COURT: All right. Wait a minute.

THE WITNESS: When?

THE COURT: "Memory storing instructions."

THE WITNESS: Yes. That would be like the hard drive would be memory storing instructions.

THE COURT: Well, you're getting instructions on how to store it on the hard drive, right?

THE WITNESS: So again, either you --

THE COURT: It would already -- it could already be on

there.

THE WITNESS: It could already be on there, or the hard drive, part of an operating system would include an update functionality so the operating system could update itself. So it could get --

THE COURT: All right. Well, what I'm trying to do is get a definition of memory storing instructions. How would you define that term?

THE WITNESS: So there are a variety of different types of memory, but I would say that it's a memory associated with the device. One way it could be is like a hard drive, something that's installed, but it could also be separate such as a CD-ROM or so on. Something that you read on the fly that contains instructions. Again, these would be the compiled computer instructions that would give it instructions for what to do.

THE COURT: Is there any difference between memory storing instructions and computer-readable media comprising instructions? I'm looking at the preamble.

THE WITNESS: Right. So memory storing functions would be an example of a computer-readable media that can store instructions, but there may be other media. Like I'm not sure I'd call a CD-ROM a memory *per se*. Well, it's a memory in the sense that it is just storing something. But it's very different than the computer memory that might be installed on

your hard drive.

THE COURT: What does non-transitory mean?

THE WITNESS: So the non-transitory just means that like it sticks around even if you turn the power off, right? So for instance, if I am running an Excel spreadsheet and my computer crashes, right, I might lose the Excel spreadsheet, the computer may not have stored all my changes to memory, but if the computer crashes and I turn it back on, the computer will still start up, right, and it will still be able to -- you know, assuming something didn't break when it crashed, it will still be able to find Excel and run Excel and so on. So non-transitory just means that, like, you know, it's in the part of the memory that's stable that's supposed to stick around even if you turn the device off and on, for instance.

THE COURT: Okay. So memory storing instructions are an example of non-transitory computer-readable media comprising instructions?

THE WITNESS: Yes. I think that's right.

THE COURT: Okay.

BY MR. HANNAH:

Q. All right, Doctor. So are the switches and the routers, looking at claim 18, are they a system that include at least one processor and memory storage instructions that when executed cause -- by at least one processor, cause the system to perform certain actions?

A. Yes, they are.
Q. So if we go to PTX-1303, Doctor, what's that document?
A. This is the cover page for a presentation from one of the Cisco Live events. I believe these were discussed before that Cisco Live are events that Cisco puts out to reach out or to interact with its customers or customer base.
MR. HANNAH: Your Honor, we'd like to move PTX-1303 into evidence please.
THE COURT: That will be admitted.
(Exhibit PTX 1303 received in evidence.)
BY MR. HANNAH:
Q. Doctor, I'd like to turn you to Page 56 of the document.
How does this inform your opinion as to whether the Catalyst switches include at least a system that has a processor and memory as shown in the claims?
A. Right. So when we talk about an operating system, an operating system is, again, stored in memory. Those are the instructions stored in, for instance, the non-transitory memory. That's what comes on every time you turn on the device, because that's what runs the device. So as we've talked about, this has a -- the switches and routers have an operating system. So those would correspond to, you know, memory containing instructions. And similarly they have processors, right. So one of the processors it has is a, what's called a programmable ASIC called the UADP. UADP stands for, if I'm getting this

right, Unified Access Data Plane. And ASIC -- oh, man, I'm blanking on ASIC because I'm stressed because I'm testifying.

Q. Application Specific --

A. Application Specific Integrated Circuit. Sorry. So you know, first of all, there are ASIC Application Specific Integrated Circuit. It's a processor. It processes instructions. And you can see that because it's sort of a preamble.

They also have other processors, what are just called CPUs, or Central Processing Units. So those are able to make use of more general instructions or more general structures. But systems have all of the above. They have memory for software, in particular the operating system, and they have processors in order to execute the corresponding instructions.

Q. Thank you, Doctor. So I'd like to turn your attention now to PTX-175.

Can you explain to the Court what is PTX-175?

A. This is a data sheet for, again, labeled Cisco Public up in the right-hand corner. Data sheets usually provide sort of a basic description of what the devices contain or how they function, again, for a customer or potential customer.

MR. HANNAH: Your Honor, we'd like to move in PTX-175 into evidence, please.

MR. GAUDET: No objection.

THE COURT: PTX-175 will be admitted.

(Exhibit PTX-175 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. Doctor, I'd like to turn you to Pages 5 and 6 of this document. We'll start with Page 5.

MR. HANNAH: And Your Honor, for your reference that's page ending in Bates No. 598.

BY MR. HANNAH:

Q. If we look at under Platform Architecture and Compatibilities section, Doctor, can you explain how this informed your opinion as to whether the Integrated Services Routers contain a system or a system that contain a processor and memory as recited in the claims for claim 18?

A. Sure. So first of all, if you look at the multi-core processors, right, again, these are the processors. The processors are what are executing the instructions, determining where to forward or, you know, determining all the functioning of the system, but in particular aspects related to where to forward or drop the packets. It also notes here that it uses -- and I believe the language is a flow processor that determines ASIC-like performance. So that's the Application Specific Integrated Circuit related to that that we have discussed before.

Again, I should also point out just --

THE COURT: What does the ASIC mean? I know what the

words are: What does it mean?

THE WITNESS: Yeah. So there are different types of processors. So your computer is built on what's called a central processing unit, or these days multiple central processing units or CPUs, and they have a fairly general instruction set, right? So you can perform all sorts of computations on your computer. You can use Zoom, you can use it for Excel, you can use it to read your court documents, right? So it has a large instruction set that makes it useful for a variety of applications. An Application Specific Integrated Circuit is a circuit that's designed -- or I would call it a processor that's designed for sort of a specific application, right? So in the context of switching and routers, like what it has to do very quickly is say, okay, I'm getting a packet, I'm looking at information inside the packet, inside the header, for instance, and I have to decide where is this packet going. And I can do that a lot better if I design a processor that's specifically designed or targeted for that application, right? So I said, look, this processor, it's not going to run Excel, it's not going to do Zoom, right? It's going to be focused on I want to figure out, look at these packets and figure out where they go next or don't go next if you drop them. So it's a processor with a specific application generally in mind and optimized for that application.

THE COURT: Which in this case is routing; is that

right?

THE WITNESS: Yes. Exactly.

THE COURT: Okay.

A. And maybe before we go on I should just point out, first of all, these are multi-core processors; that is, like in the old days when I was a kid you were lucky to get like one CPU. Like one processor on your chip. These days things have gotten smaller, more complicated, so now you get multiple processors, multiple CPUs, and they call it multi-core, right? So it's like several cores, several processing components on a single chip. And again, with regard to memory and instructions, it talks about here -- I think above this section it also talks about this is designed to run Cisco iOS XE. I think it also says sort of in the second box, and I think it also says above this table in the documents as well.

THE COURT: Well, where it affects my office on a daily basis is as soon as we figure out how to use whatever Microsoft's newest system is, it changes.

THE WITNESS: That is true.

THE COURT: And when they change it, it makes it more difficult to do the simple things. Every time they add an app it makes it harder to --

THE WITNESS: To just do your Microsoft Word. I know.

THE COURT: Right. Okay. And I think I understand what you're talking about here. This is a special processor

that's designed to perform either one or a limited number of functions.

THE WITNESS: Exactly.

THE COURT: Okay.

BY MR. HANNAH:

Q. All right. Doctor, if we turn to the next page of this document which is Page 6 ending in Bates No. 599, can you explain how this informed your opinion as to whether the Integrated Services Routers contain a memory as recited in claim 18?

A. All right. So this discusses actually two different types of memory, flash memory. That would be like typically the way your hard drives are built these days, DRAM stands for Dynamic Random Access Memory it. I've got that right. That typically might be the memory that's being used by applications or so on as they're running within your computer. But in particular, like both of these, and the flash memory in particular, shows these devices have memory for storing instructions.

THE COURT: Wait a minute. Now DRAM is not on my list.

THE WITNESS: Is not? Oh, sorry.

THE COURT: It's not on the list of abbreviations. DRAM stands for what? Dynamic what?

THE WITNESS: Dynamic Random Access Memory.

THE COURT: That means -- dynamic means changes

through --

THE WITNESS: Yeah, it means changeable. So typically like the DRAM, if you're running one application, some of the information about that application might be held in the DRAM, whereas then if you like turned off that application and ran a new application, then that memory would get reused to hold other application information.

THE COURT: In other words, that's what would enable you to introduce a new set of rules and/or drop an old set of rules?

THE WITNESS: The DRAM would certainly, I think, be used in any sort of system that was doing that, yeah.

THE COURT: All right.

BY MR. HANNAH:

Q. All right, Doctor. Thank you. And I'd like to turn to PTX-1313. If we look at PTX-1313, can you explain what that document is, please?

THE COURT: Just a moment. Let me find that.

MR. HANNAH: Yes, Your Honor.

THE COURT: All right. I have it.

A. So this is an overview document for the ASR, which is -- or sorry, ASR routers that we had talked about. So this is just an overview document, again, providing information to present to potential customers and so on. It looks like sort of talk slides.

MR. HANNAH: Your Honor, at this point I'd like to move PTX-1313 into evidence.

MR. GAUDET: No objection.

THE COURT: That will be admitted.

(Exhibit PTX-1313 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. Doctor, I'd like to turn your attention to Page 18.

MR. HANNAH: And Your Honor, it shares the same corresponding Bates number at the end as 18.

THE COURT: All right.

BY MR. HANNAH:

Q. Doctor, can you explain how this informed your opinion as to whether the Integrated Services Routers include or are a system that includes at least one processor and memory?

A. Sure. So if we look at the top it's talking about CPU in that central processing unit. That's sort of a standard multi-purpose processor. And you can see that all of these devices contain processors. In fact, most of them contain multiple processors; that is, multiple cores within a single process unit. In terms of memory, you know, boot flash out is, what I would assume both the memory and boot flash would contain the operating system, and particularly the boot flash. And we can see, in fact, the operating system named a couple of lines down it's the Cisco iOS XE OS. So again, OS here stands for

Operating System. So again we can see that these devices have the operating system which would be stored in memory. So it could run when the system was ready to go.

Q. Doctor, with that I'd like to turn back to the claims, and as you've discussed earlier, claim 18 recites a system, a process, or a memory, and then claim 19 recites the computer-readable media. Because we're able to prove that there's a processor and memory, does that also mean that claim 19 is met, the computer-readable media as recited for the switches and the routers?

A. Yes, I would say this part of both claim 18 and 19 are met.

Q. Can we check the box?

A. Please do.

Q. All right. I'd like to turn your attention to the next element, which is the receive element as recited. Do you see that, Doctor?

A. Yes.

Q. Can you explain for the Court what's required by this element?

A. Well, so here we're talking about receiving packets. And again, all of these switches and routers receive packets either from other devices inside the network, other gateway routers or so on, or from, or from, you know, the devices themselves, the users that might be sending packets. And here there's some language which will be discussed further in some of the other

elements below about a first portion and a second portion of packets. And these will correspond to packets that are either going to be blocked or allowed according to corresponding rules of the switches and routers.

Q. If we take a look at the demonstrative that you showed before earlier, can you map this to the claim element, the receive claim element and what we're talking about here?

A. Certainly. So what we're going to show is that these switches, according to certain rules -- and the same for the routers -- can determine whether or not packets are allowed to continue on to a permitted network or, I don't know, might be stopped or rejected because they're going to or coming from some sort of protected network.

Q. I'd like to show you PTX-1276.

So Doctor, can you explain what is PTX-1276?

A. So this is a software system functional specification. You can see it's crossed out iOS XE and put in Polaris. Polaris is, I guess, is an internal code name for Cisco's operating system, IOS XE. And you know, the document describes itself. It explains that it defines the engineering requirements as well as the system architecture for an involved iOS XE operating system.

Q. Doctor, I'd like to just look at the bottom. This says there's a copyright of 2011, but then it says that the initial version of this document was 2013. Can you explain the discrepancy here and what you've noticed in the Cisco

literature?

A. Yeah. So hopefully this is coming in. My Internet got a bit unstable for a second.

But my understanding based on a number of the documents that I have looked at, is that sometimes Cisco documents were put on just some sort of boilerplate, so like someone I guess somewhere had developed a boilerplate document that people had used whenever they created a new document. And you know, there was, I guess, appears to be one going around that said copyright 2011. In a case like this, one where you can actually see the revision date, I would trust the revision date rather than the copyright on the bottom, since it appears to just be a, you know, sort of a blank boilerplate that it was started from.

Q. And when you have these types of system functional specifications, you would look to the latest revision as the, for the appropriate date of the document?

A. Yeah. For the, that would be -- the latest date would be the date on which, you know, this document in its current form stood.

Q. Thank you, Doctor. So if we turn to Page 12 -- I'm sorry, 216 of this document?

MR. HANNAH: Your Honor, the Bates label is also 216. It has the same corresponding page number.

THE COURT: Okay.

BY MR. HANNAH:

Q. Can you please explain what's being shown here, Doctor?
A. Yeah, so I think this chart gives sort of a very key sort of high-level way of understanding what is going on here. Or what is going on in these switches. So you see at the bottom, it says like packet comes in. Okay. So first, like most importantly I guess for this claim element, you know, packets come in, and these devices receive packets, and that's really maybe all we need for the claim element right now. But just as a precursor of what's to come, there are various sorts of rule sets that we can see. And you know, so if you look at the left, you can see it talks about there's all sorts of acronyms, and I don't want to get into those acronyms now, but those correspond to different rules or rule sets. And you know, if you don't pass the rules, you can see the Deny and the arrow to drop the packet, right? So if you fail on one of these rules, you're going to get denied and the packet will be dropped, but if you pass all the rules, then eventually the packet will go out.

And if you look at the top, I guess it says Forwarding Lookup. The forwarding lookup tells you, you know, this is where it's going to go assuming the packet makes it all the way out.

Q. And does this -- because this is talking about operating systems of both the routers and switches, does this show that the routers and switches both receive packets that come in?
A. Yes.

Q. In the middle it says "Drop the packet." Does that also show that the routers and switches are able to block packets?
A. Yes.
Q. So Doctor, based on your analysis of the products and the documents, and turning back to the claims, do the switches and routers meet the first receive element of claim 18 and also the first receive element of claim 19?
A. Yes, for both claim 18 and 19 they meet the element and we can check the box.

MR. HANNAH: And I believe I already did this, but Your Honor, I'd like to move in PTX-1276 to the extent I haven't done so already.

THE COURT: PTX-1276 will be admitted.

(Exhibit PTX-1276 received in evidence.)

MR. HANNAH: Thank you.

BY MR. HANNAH:
Q. Now turning to the next element, which is "responsive to a determination" do you see that?
A. Yes.
Q. Can you explain to the Court what's required of this element?
A. So what's required here is that you can see that there's a first portion of packets that correspond to criteria specified by one or more rules. So in particular, the rules that we're going to be talking about here in my example, my exfiltration

rules might be rules that say, okay, this user seems to be doing something suspicious. I might have a rule put in place that says, look, I'm not going to allow this user to access certain locations, you know. A possible response might be, say, well I'm going to restrict this user from accessing certain parts internal to my network because I'm suspicious they're gathering information from finance and they shouldn't be gathering information from finance, but while we look into this, I want them to continue their work. So they can still use the Internet, they just can't access finance. All right. That would be the sort of rule that you might set up to deal with an exfiltration scenario. All right. So the idea is that, you know, when you look at these packets, if you find that someone's trying to use something they're not supposed to use, you might block them, right? You would say I don't want this person accessing that information at this time.

So this could be a data transfer from a first network to a second network. So that might be internal subnetworks, right, where, again, finance has their own subnetwork and the human resources department have their own subnetwork inside the larger network that belongs to the business. It might be that you might prevent people from inside your network from sending information out to certain other external networks because you're worried that they're shipping information out that they shouldn't be. In all these cases, we're talking about rules

that are going to block types of transfers from one network to another network.

Q. And again, this element is identical for both Claims 18 and 19?

A. Yes. In particular we could think of the case here where you're trying to block information from a user, say, going out.

Q. So if we look at your demonstrative, at what point are we talking about here for this element?

A. So you could have information in your internal network and your switch will say okay, if it's permitted, you're allowed to go to that permitted network, but if instead you're trying to send information out and it's a protected network or a network covered by the rules that you're not supposed to send information to, that packet would be dropped.

Q. All right. Doctor, I'd like to turn your attention to PTX-576. Can you explain what this document is?

A. Sure. This is a data sheet describing Cognitive Threat Analytics, or CTA. And I believe we've discussed briefly how that's related to this, the StealthWatch and monitoring by some of the Cisco products.

MR. HANNAH: Your Honor, I'd like to move PTX-576 into evidence.

MR. GAUDET: No objection.

THE COURT: That will be admitted.

(Exhibit PTX-576 received in evidence.)

BY MR. HANNAH:

Q. Doctor, I'd like to turn your attention to Page 3 of this document.

MR. HANNAH: Which, Your Honor, is the page ending in Bates No. 991.

BY MR. HANNAH:

Q. The top table there where it says "data exfiltration", can you explain how this informed your opinion as to whether the Cisco technology can block data exfiltration?

A. Certainly. So again, data exfiltration is the example using throughout here, and data exfiltration, as it says, like this is the part that's doing the analysis that says a-ha, I seem to have discovered something that's odd or wrong, so based on the fact I've seen this sort of odd behavior, there are going to be certain types of data transfers that I want to stop, maybe from some specific user who you think is behaving potentially badly. And so this is what is going to lead to setting up a sort of quarantine or the rules that switches and routers have to follow, and these are the rules that I'm talking about in the claim.

Q. And when it says that they can do data exfiltration even in HTTPS-encoded traffic without any need to decrypt transferred content, can you explain what that means?

A. Yeah. This relates to the judge's questions earlier about, you know, data exfiltration. What if the content is encrypted

so you can't even tell what information someone is trying to sneak out? And again, the CTA can look at data exfiltration even if it's in encoded traffic without decrypting it. And my understanding it's based on, sort of at a high level, some of the ideas the Judge was describing before where you might base it on the quantity of information that you see as well as the location of the information, where it's coming from, rather than the actual contents of the information itself when you make this decision that there's an exfiltration threat.

Q. Okay. Doctor, I'd like to show you PTX-1262.

Can you explain to the Court what this document is?

A. This is another Cisco document, a general document describing their 9000 switch series.

MR. HANNAH: Your Honor, we'd like to move PTX-1262 into evidence, please.

MR. GAUDET: No objection.

THE COURT: That will be admitted.

(Exhibit PTX-1262 received in evidence.)

MR. HANNAH: May I proceed, Your Honor?

THE COURT: Yes.

BY MR. HANNAH:

Q. If I can go to Page 77 of this document, which has the corresponding Bates No. 999.

If we look under the Policy and ACL paragraph, can you explain how this paragraph informed your opinion in regard to

whether the Cisco Catalyst switches and routers meet the claim element?

A. Yeah. So again, certainly this is showing -- so ACL stands for Access Control List. And that's how these -- one of the ways these rules get implemented. So here, I think the key thing that I'll be talking about when I get into some of the details are that one of the things that it uses are these scalable group tag, SGT, which is in the middle of the paragraph.

Yeah, starting at special tags I guess, if you can highlight that.

So it's going to use as part of the ACL infrastructure as part of the rule list that's going to say one thing that can happen is that you're deemed a security threat, you might get a special tag, right, a special label. So all your packets are going to be labeled saying this one needs some maybe extra examination or some extra consideration. The idea of this Scalable Group Tag is -- and this is how it implements what we've been calling the quarantine. So if you've found a user that's suspicious you might say, okay, I'm going to apply this Scalable Group Tag, in particular a quarantine tag, and then I'm going to use that as part of the rule which means that I'm going to look more closely at where this packet is coming in and coming out and whether I'm going to allow or block it. And there's other language in the paragraph that talks about the

processor that we've been talking about for doing these rules like the UADP, which handles the traffic classification and policy enforcement.

Q. If you look at the last line, Doctor, it talks about "Examples include permit, deny." Do you see that?

A. Yes. Exactly. So the sentence before says "UADP can then apply appropriate policies configured by the network administrator. Examples include permit, deny" and so on. So this is precisely it: Based on the quarantine, if you've decided a user is a potential threat, in particular there's an issue perhaps with exfiltration, you can instruct, you can create rules that instruct the switches and routers to permit or deny traffic going to or from certain places for that particular host.

Q. All right. If we can go to PTX-1280?

Doctor, can you explain what PTX-1280 is?

A. So this is another white paper. So white papers are, again, public-facing documents that describe a technology that you'd use to present to a slightly more technical level. And this is talking about how you can use the network, how you can use switches and routers to provide access to certain resources or not.

Q. When it says "Network as a sensor," what does that mean?

A. That's this entire idea that, you know, that Cisco has been talking about in its documents, where the idea is the network is

both gathering information in order to decide and implement security rules, and then going back and implementing those security rules on the switches and routers to prevent bad things from happening.

MR. HANNAH: Your Honor, at this time we'd like to move in PTX-1280 into evidence?

MR. GAUDET: No objection.

THE COURT: That will be admitted.

(Exhibit PTX-1280 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. If we could go to Page 21 of this document, and this corresponds to also Page 21 in the Bates label.

Now if we look at the last portion of the document, Doctor, can you please tell the Court how this informed your opinion, in particular the last line of that first paragraph?

A. Sure. So this is maybe a bit, getting into a bit more technical level. And again, this is how it implements the idea of the quarantine. So we've seen SGT previously. So SGT was Scalable Group Tag. So the idea is you're going to tag information related to a user depending on, you know, the security considerations. So here what it is saying is that they're changing the Scalable Group Tag from a user from 4 to 255, and that's the quarantine Scalable Group Tag, right? So by changing this tag for this user from 4 to 255, what it's saying

is that the packets related to this user, this address, are going to be provided this label, 255, which says that there's additional restrictions that have to be considered. And you can see that above.

So in the example they're using above, says there that the endpoint will continue -- sorry, just the paragraph above. The Rapid Threat Containment.

So the Rapid Threat Containment, right -- again, this is for Rapid Threat Containment. The idea is that you've seen a possible threat and you're trying to shut it down as soon as possible; in particular you're trying to shut it down, the threat, before anything bad actually happens or as early as you possibly can, okay?

THE COURT: Is that 4 to 255, does that mean 4 packets to 255 packets?

THE WITNESS: No, no, no. That's just an ID number. So for instance let's say that, like it may be that in your courthouse, right, that judges have access to all the rooms in the courthouse, right? So maybe on their security tag their tag is labeled 1, which means they have access to everywhere. But someone else's security badge maybe they don't have access to everywhere. They have access to lots of places, but they can't, for instance, just go into a judge's chambers, right? So their access they might -- their badge might be labeled with a number like 3, right? And 3 says, is a shorthand for, well, there are

certain places you can go, things you can do, but other things that you can't.

THE COURT: Okay.

THE WITNESS: So that's what the tag is. When it changes from 4 to 255, that's like saying, you know, maybe you found an employee who had access to a lot of rooms in the building, but now you're concerned that their security, there's a security issue. So you may change their access like you may change their badge. Instead of like a 3 badge which gets them in almost everywhere, you may give them a lowered-numbered badge or a differently numbered badge like 5, which says, okay, you can go to the places that you need to go, but you're restricted from going in some of the more important places, at least for now.

That's the same idea as this tag. So this tag is sort of saying that packet's going -- related to this user or this address, they have a different security level associated with them. So you can think of the 4 and 255 as being like security levels or security shorthand names.

BY MR. HANNAH:

Q. Is that also illustrated in that second line which says that it will limit the endpoint's network access?

A. Right. So the idea is that in here, it says up at the top, "The endpoint continues to be operational and in the employee VLAN." So you're still giving them some rights. They can still

do some things, right? But the fabric edge devices will then download" -- I'm going skip the SGACL. That's security. Or Scalable Group ACL -- "permissions specific to SGD 255." So that's like saying, oh, somebody's been given a security warning label, they have been labeled a 255, there's going to be special permissions for them, certain things they can and can't do. And in particular, as it says here, it will limit the endpoint's network access.

So the idea is that hopefully in terms of exfiltration, you've stopped the person and you said okay, look, right now you're not allowed to use certain types of network operations because maybe you're trying to send data out that you're not supposed to do, we're going to check it out and hopefully you've stopped it or ideally the goal was you stopped it before it happened. And you can see down below, right, like the sorts of things that happen is that you get more deny operations.

Q. And by deny operation is the way that the switch or the router will actually block the traffic; is that right?

A. Yes.

Q. All right. Doctor, I'd like to take to you PTX-563.

Doctor, what is PTX-563?

A. That's another Cisco Live presentation document. And this would be outward-facing to the public.

MR. HANNAH: Your Honor, we'd like to move PTX-563 into evidence, please.

MR. GAUDET: No objection, Your Honor.

THE COURT: All right.

(Exhibit PTX-563 received in evidence.)

BY MR. HANNAH:

Q. Dr. Mitzenmacher, I'd like to turn your attention to Page 119.

MR. HANNAH: For your reference, Your Honor, this is page beginning in Bates No. 414.

BY MR. HANNAH:

Q. Doctor, can you explain what's being shown on this graph and how it relates to the claimed element that we've been discussing for the '193 patent?

A. This might be an example of what could occur with, again, if you look at the top it says "Rapid Threat Containment". Again, you've noticed something and you're trying to contain it as quickly as possible before the damage is done. And so you can see on the left, the information from the Cisco StealthWatch has, in this display, suggested that a supplier be quarantined, right? So in here, in this instance, that will correspond to a rule marked by the red arrow which I would interpret as saying that the supplier is no longer allowed to access certain shared server information, right? That it's like you're not allowed to pull information from there because you're worried that you may be gathering information you shouldn't.

MR. HANNAH: And if we go to the next page, which is

Page 120, it also, Your Honor, ends in Bates label 415.

THE COURT: I'm sorry, what's this number?

MR. HANNAH: It's the very next page, Your Honor. It is the page ending in Bates No. 415.

THE COURT: Okay.

MR. HANNAH: It's a build from the previous graph.

THE COURT: All right.

BY MR. HANNAH:

Q. Doctor, can you explain what's being shown here?

A. Right. So you can see that what's happened -- or because of this is, you know, this next slide, you've changed the authorization. So now that supplier is I guess marked as being in quarantine, right, and because of that, you know, they're not going to have access to the shared server, to employee information and so on. But while they're on your system you may still how them to access the general Internet. And so the idea of this version of containment, right, is that you've decided, well, I'm going to allow them to do normal Internet-type things, but not allow them to access internal information. There are other situations, you could reverse it the other way where you would say, well, I'm not going to allow them even out to the Internet or you could say they could do some internal job functions, but I'm not going to let them work with the Internet outside. Here, this example of the policy is that they're allowed to use the Internet but not to gather or pull

information from these other sources.

Q. So when we're looking at this diagram, does the red represent that the quarantined computer not have access to those different resources that are being shown?

A. I believe that's my understanding, yes.

Q. And if we map this to your demonstrative, would the red be the protected network and then the green checkmark to the Internet would be the network that is permitted for that laptop, the quarantined laptop to access?

A. Sure. Under that interpretation, yes.

MR. HANNAH: All right. Your Honor, at this point I would like to show the Doctor some source code, and so in terms of the procedure, I believe that we're going to mute or put the people on the conference line into another room or something of that nature?

THE COURT: All right. Well, we instructed the people observing the audio the first day to mute themselves. What counsel is requesting at this point is equivalent of having a bench conference if we were all sitting in the court. In other words, I would ask the attorneys to approach the bench so that neither the jury, if we had a jury, or the specific spectators would hear what we're saying, and usually has to do with evidentiary issues. So what I'm going to do is go ahead and take our luncheon recess, and when we come back -- I'll ask everybody to return at 1:55 -- and we'll have our bench

conference. So we'll be recessed until 1:55.

(Recess taken from 12:56 p.m. to 1:55 p.m.)

THE COURT: All right. For those of you who are observing the proceedings on the audio, we are now going to take a break to consider some evidentiary issues and also to consider, for the Court to consider in-camera, we call it, some evidence that's confidential. And I'm not sure how long this will take.

MR. HANNAH: So Your Honor, I believe I misspoke. Apologize for that. But what we need to do is -- or what we're hoping to do is just to seal the courtroom. There's no dispute in terms of what's being offered, it's just to seal the courtroom because I believe Cisco has requested that we seal the courtroom for any time that we are going to display source code. And so that was what I was trying to get at. There's no evidentiary dispute as to what's being shown, it's just the fact that we're showing source code.

THE COURT: All right. We'll mute the audio.

COURTROOM DEPUTY CLERK: Done.

THE COURT: All right.

MR. GAUDET: And Your Honor, this is Matt Gaudet. If I may make one other point? As far as everyone that should now be able to watch this is certified under the protective order, if you will, to see source code with just one exception, and that is Centripetal's corporate representative, Jonathan Rogers

would not be qualified under the protective order to see what Cisco considers to be truly its crown jewel, its source code. So we would ask that Mr. Rogers be sealed out only for this small portion that the source code is discussed.

MR. HANNAH: And it's my understanding he has left the room and he will not be watching source code until we tell him to go back into the room.

MR. GAUDET: Terrific. And I understand he's the only non-expert or non-lawyer that's still participating, and as long as that's the case, that should take care of it.

THE COURT: All right. You may proceed.

MR. HANNAH: Thank you. May it please the Court.

BY MR. HANNAH:

Q. Doctor, I'd like to show you PTX-1849, and if we could, this is the source code. And if we go to page, it'll be Page 9, Your Honor, of this, and it's going to be beginning in Page No. 009 as well.

THE COURT: All right. We're on PTX-1849. You may proceed.

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. Doctor, looking at PTX-1849 and Page 9, is this a portion of the source code that you relied upon for your opinion?

A. Yes.

MR. HANNAH: Your Honor, we'd like to move in

PTX-1849. And I believe we're going to move in the cover page just to show that it's PTX-1849, and then the particular page numbers that we actually discuss today and so that would --

THE COURT: Give me the Bates number.

MR. HANNAH: Yes, Your Honor. It's zero -- the first one is 001, and then the actual page is 009.

MR. GAUDET: Based on the procedure, we have no objection.

THE COURT: All right.

(Exhibit PTX-1849 received in evidence.)

THE COURT: Well, we're now looking at 009.

MR. HANNAH: That's correct, Your Honor.

BY MR. HANNAH:

Q. All right, Doctor. Can you explain what's being shown here on the screen?

A. So you'll see that this is a page of code. In fact, up at the top that's the directory which was sort of the location of where the code lived and what the name is for the code. You can see that this code relates to the ISE, the Identity Services Engine, and in particular is under a directory ANC. That stands for, if I'm remembering right, Adaptive Network Control. Adaptive Network Control is where the code and the system framework for doing this sort of quarantine is located.

Again, the quarantine, just to remind you, we discussed a bit last, before lunch, that involved changing the Scalable

Group Tag. The example was changing it from 4 to 255. That's like giving, sort of resetting the ID to a different security level for that user. And you know, the quarantine involves that Scalable Group Tag as well as some associated policies or rules which are implemented by what are called ACLs or Access Control Lists.

So if we go now and look at this page of code, this is just to show that this is, you know, one of the places where this sort of quarantine code lives.

If we could, I guess, highlight from -- yeah, there is fine.

There are certain actions that can take place, and here it's recording it into a file, but it shows that one of these actions that can take place is this quarantine. A fact where the quarantine is as we've described or as shown in the other documents what this quarantine is set to do, is to limit the network access of a particular user or group of users.

BY MR. HANNAH:

Q. And just to be clear, the switches in the routers will enforce the quarantine; is that correct?

A. Right. So what happens is they get a message and are told this is a quarantine. So this is a rule action that gets implemented to say, okay, well, from now on when I see, you know, packets related to this user I am going to have to consider or apply the Security Scalable Group Tag.

Q. All right. Doctor, I'd like to turn to Page 21 of the source code.

MR. HANNAH: And Your Honor, that ends in Bates label 021.

BY MR. HANNAH:

Q. If we can blow up the top? Doctor, can you explain what's being shown here?

A. So this is code that relates to the Catalyst switches, and after Catalyst switch you can see the letters ACL. And again, that's Access Control Lists. And these are, again, the rules that are used to determine whether a given packet is going to be allowed to proceed or not proceed, to continue or be blocked. And the ACL, or Access Control List, is how these rules are implemented down at the switch level. So part of what the switches get told is here are the rules for how to deal with these packets.

Q. If we could look at lines around 585? Can you explain what's being shown here in terms of the source code that's actually on switches?

A. Yes. So this is in a certain state where there's going to be a policy update. So if you look at, for instance, at 594, there is talking about a policy update, policy install. And just at high level, the idea of this code is this code is managing or handling issues or changes in these Access Control Lists. One of the places where such a change might occur or

would occur is when a subject is being quarantined and it might require an update or a change in policy. And again, it's -- these would be rules that would be taken in or received by the switch so that they would know how to respond and know what packets needed to be blocked or and which ones can be permitted.

Q. And Doctor, if you look at Line 588 there's a line there that's looks like it's written in English, and it's a little bit of a different color. Can you explain what this is in source code?

A. Sure. So first of all, that is written in English, and one of the things that you can do in source code is leave what are called comments. So comments are things that the programmers, the engineers, put into the code so that later people can go back and read the code and maybe get some insight or some suggestions as to how the code was functioning. Essentially it's way of leaving, you know, commentary, generally some tips or explanation of how code is functioning. So, again this would be written by the engineers or the programmers themselves.

In this case, you can tell it's a comment because in this language, this code is written in the C programming language, the comment /* at the beginning sort of denotes that there's a comment here. And you know, here it's just saying the drop label and the LE table to drop traffic for the interface. This is just showing something that we already know or have seen from the various documents: The switches can be programmed to drop

traffic along various input or output situations. Here it's doing it in the context of an update. And there were other ways as we've seen in the documentation where we'll drop packets in response to not passing certain rules.

Q. All right. Thank you, Doctor.

I'd like to turn your attention to Page 228 of the source code.

MR. HANNAH: First of all, Your Honor, I'd like to move in Page 21 of the source code that we just talked about.

THE COURT: All right. Page 21 will be admitted.

(Exhibit PTX-1849, Page 21 received in evidence.)

MR. HANNAH: Now I'd like to turn your attention to Page 228. It ends in Bates No. 0228. Has the same corresponding Bates number, Your Honor.

THE COURT: 228?

MR. HANNAH: Yes. 228.

THE COURT: Last three numbers are 228?

MR. HANNAH: Correct.

THE COURT: Okay. I've got it.

BY MR. HANNAH:

Q. Doctor, I'd like to show you -- first of all, Doctor, can you explain what this is and confirm that this is source code that you relied upon in providing your opinion?

A. Yes. This is source code I'd examined and discussed in my

report. And to the left at the top I guess we can see this is part of what was called the CTA, which I believe was Cognitive Threat Analytics, right? And so this was the question of, you know, just to provide an example, how is it that the routers or switches get these rules? And you know, where might they come from and what are they, what is their purpose? And here I'm going to show some of the descriptions for sort of events that can occur within the Cognitive Threat Analytics which would cause it to take some sort of corresponding action.

MR. HANNAH: Your Honor, at this point I'd like to move Page 228 of the source code into evidence.

MR. GAUDET: No objection.

THE COURT: Admitted.

(Exhibit PTX-1849, Page 228 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. So Doctor, if we turn to Line 1089, can you explain what's being shown here and how this informs your opinion as to the "responsive to" element which talks about the criteria specified by the "one or more packeting rules that are configured to prevent a particular type of data transfer from a first network to a second network"?

THE COURT: You mean line 1089, I guess?

MR. HANNAH: Yes, Lines -- yes. Yes, Your Honor.

1089.

A. All right. So this you can view as, I guess, a form of metadata. In the code it's describing things that it may have found, and you know, the concerns and so on that would cause these quarantine rules to come into effect. So you can see here in the description it says that an outbound HTTP GET to a remote certainer was detected. So what's going on here, HTTP I think you heard about before, Hypertext Transfer Protocol, that's just the protocol we use to receive information from the web and also to put information out on the web if we're a server. And what this is saying is like the analytics have discovered some suspicious activity related to a quantity or a quality of GET information; that is, that it has done some of these transactions across the Internet which looks suspicious, and it's giving us a text description of what it was that was potentially suspicious about this, that -- you know, malware will sometimes use these types of commands to check in with what are called command and control servers, okay? So command and control servers are the idea that there is some other server out on the Internet that's now directing or is taking control of part of your computer and getting your computer to gather information, potentially proprietary or secret information, and sending it back out to them. And you can see at line 1092 it discusses this as exfiltration.

So it would be this sort of observation, right, this sort

of determination which would lead to the quarantine rules that we've been discussing; that once -- this is the observation phase, and it would lead to a corresponding action phase where you would say, well, I've got to watch what that user's doing and put a stop to something that might potentially be going wrong right now.

THE COURT: So this is where somebody tries to invade the network?

THE WITNESS: Yes. And in particular to put some sort of code on your machine that it can use to gather and extract, as they call it, exfiltrate information from inside your network. And this is saying they have seen some activity that's very suspicious in this regard.

And if we look at the bottom, I think there are similar texts regarding, you know, what's called POST operations. I think starting at 1111, okay. So you know, GET is a type of operation where you're trying to get information, POST is where you're sort of sending out information. And again, that can be done through the Hypertext Transfer Protocol, HTTP. And here it's saying that, again, the system has found some sort of suspicious activity that might be a sign that it's trying to exfiltrate data; that is, trying to send data out when it should not, and again you can see sort of the category at Line 1114 as they view this as a potential exfiltration event. And they would then use this information, use these observations

to decide if they needed to change the rules, change the system to induce this quarantine that we've been discussing.

MR. HANNAH: Your Honor, we're done with the source code for this element and we can open back up the courtroom at this time.

THE COURT: All right. You may resume.

MR. HANNAH: Thank you, Your Honor. Thank you, Lori.

So Your Honor, I would like to show the Doctor some deposition testimony, and I believe earlier you said that you wanted to either have it played. Would you like to have it played at this time, or we have a slide of it as well that we can just read into the record. We can do it either way. We also have a short clip that we can show you. We have managed to be able to -- we can show it to you on video or we can summarize with a slide.

THE COURT: Well, what I want to do is avoid a duplication of effort. I don't want to look at it one time, whether it be by slide or video, and then have to go through it again if we can avoid that. But I think you and perhaps the witness are in a better position than the Court to determine whether it would be more understandable if we looked at the clip or looked at the slide. That's up to you.

MR. HANNAH: All right, Your Honor. With that, I think it would be better to look at the slide.

So we can show the next slide.

THE COURT: All right.

BY MR. HANNAH:

Q. So Doctor, can you please inform the Court how this informed your opinion with regard to this element? This is from Page 48, Lines 21 through Page 49, Line 16.

THE COURT: Okay. Now let's get this down. This is page what? 49, did you say?

MR. HANNAH: 48, Line 21 through Page 49, Line 16. And in your binder it's the first deponent that you'll see in the binder. It's Cernohorsky.

MR. GAUDET: Your Honor, this is Matt Gaudet. I've got a logistical question when you're ready for it.

THE COURT: You said in my binder it's what now?

MR. HANNAH: In your deposition binder it's the first --

THE COURT: Is the deposition binder different than the one we've been looking at?

All right. Here is the deposition summary. And you've got several excerpts from the deposition. This would be among the excerpts, I assume?

MR. HANNAH: Yes, Your Honor.

THE COURT: Page 48.

Well, this is a portion of 48.

MR. HANNAH: Correct, Your Honor. It's a limited portion. And the Doctor is going to explain what this means.

THE COURT: All right.

MR. GAUDET: Your Honor, if I might just raise one quick issue, which is this -- and I imagine this will be the case -- this is the portion of their designation. Across a lot of these there were a lot of counter-designations which wouldn't be included here. And I guess the question is just how we go about being sure that all does find its way into the record if they're going to just put up portions that sort of weren't identified to us ahead of time.

MR. HANNAH: What we would suggest, Your Honor, is we would just move in the entire deposition that's in your binder as PTX-1898.

THE COURT: No, we're not going to put the whole deposition in the binder. That would make the whole deposition part of the Court record, which is what we're trying to avoid.

MR. HANNAH: Correct.

THE COURT: Because I don't want something in the record that the Court doesn't have an opportunity to look at. So we're just going to put the slide in the record.

MR. HANNAH: Very good.

THE COURT: And if there's a counter-designation to the slide then the defendant can put that in there.

MR. HANNAH: Very good.

THE COURT: And you can just compare the counter-designation with their designation and put in your

counter-designation when it's time for you to examine the witness, Mr. Gaudet.

MR. GAUDET: Thank you, Your Honor.

THE COURT: All right. So this is just a slide. All right. You may proceed.

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. Doctor, can you please explain for the Court what this is showing?

A. Yeah. So if we read this, you know (inaudible).

THE COURT: So "What input does it take?" What is "it"?

A. Here it's talking about parts that we were just looking at before. StealthWatch, cognitive (inaudible) information.

THE COURT: Well, what is "it"?

A. The reason to show this, Judge, I would say, is to show just that it's getting information about these HTTP requests. So we saw in the code that it was saying, hey, we've seen some suspicious HTTP, Hypertext Transfer Protocol, activity related to GETS or PUTS that may relate to exfiltration, and the purpose here of this deposition testimony is just to confirm that this is the sort of information it gathers or receives that we've already seen discussed or confirmed in the code.

MR. GAUDET: Your Honor, this is Matt Gaudet. I apologize. Our audio cut out when Dr. Mitzenmacher was

beginning that answer. I don't know if others had that same problem, but unfortunately we missed the answer to the Court's question of what the "it" is. I don't know if we're the only ones having the audio problem though.

THE COURT: Well, why don't we -- let me read this before we do anything else.

All right. Well, there's no way the Court could read that question and answer and have any understanding of what it means without the explanation from Dr. Mitzenmacher. Is the "it" in the first question StealthWatch implementation? Is that what "it" means?

THE WITNESS: I believe so, yes.

THE COURT: All right. Well, what is he saying here?

THE WITNESS: So what he's saying is that what this receives is, as he talks about it, is network metadata, NetFlow, which can include various sorts of information which he's describing, like the source and destination of a communication, the volume of bytes transferred. The judge has discussed the idea of the volume of information, and other characteristics. And then the weblogs, which is, again, the source destination of the communication, the metadata of the communication.

What's next asked is one of the inputs also URLs? The answer is that would also be within the weblogs. A URL is part of the request, the full HTTP request, and so on.

And again, the purpose of this is just to confirm what

we had seen in the code and what we had seen at a more high level in the descriptions that one of the things it's receiving is information about these HTTP, Hypertext Transfer Protocol transfers, and in particular, as we've seen in the code, it's looking and determining is there a potential for exfiltration here that might cause us to set up a corresponding rule in order to prevent that from occurring.

THE COURT: All right. Now, this is the problem that I foresaw in trying to introduce these depositions, and that is that the language which the witness uses is such that there's no way for the Court to understand what he means without the doctor's explaining it. So if you've got what you want on slides, then the Court will admit the slides which will be part of the record and identified in the doctor's testimony. But to try to introduce the slides separately, these are the kind of questions and answers that those depositions contain, I don't think they would be of much use -- I don't think they would be of any use to the Court. So let's proceed and look at the slides.

MR. HANNAH: Thank, Your Honor. We will.

BY MR. HANNAH:

Q. So Doctor, let's turn back to the claims. And can you explain based on the evidence that we saw before lunch and the corresponding source code and the testimony how that matched to the different claim elements of both Claims 18 and 19 for the

routers and the switches?

A. All right. So it says here "Responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet filtering rules configured to prevent a particular type of data transfer from the first network to the second network, wherein the indicates data indicates that the first portion of packets is destined for the second network."

So here, what we've seen is, that for instance, in an exfiltration attempt, a user or network may be passing on, a user may be passing data out of the network to another location to another network that is not supposed to be getting that information. So "responsive to a determination," right, is going to be this determination is going to be the quarantine rule, right? So it's going to be that there's a ACL associated with the --

THE COURT: A what?

THE WITNESS: Sorry. An Access Control List, a rule associated with the quarantine that says, hey, you cannot actually send this out of this location, and it comprises data corresponding to criteria specified by one or more packet filtering rules. Again, here, the criteria would be this is a location that you're no longer allowed to access because of the quarantine, you're no longer allowed to send information there because of the quarantine, and that is configured to prevent a

particular type of data transfer from the first network to the second network. Again, we see that's the purpose of the quarantine. It's based on the idea that there's been suspicious activity noted in terms of various gathering, hoarding, collecting or even sending of information, and so the idea is that you want to put an end to that particular type of data transfer. "And wherein the data indicates that the first portion of packets is destined for the second network," again, this rule would be based on a specific end location. So it's looking in the packet, it's saying I see in the packet that you're trying to send information to this other network, to this other location, and that specifically is what I'm going to try and prevent.

BY MR. HANNAH:

Q. And when it talks about the particular type of data transfers, does that relate to the HTTP GET and HTTP POST that you explained?

THE COURT: Don't use those abbreviations, please, in your question.

MR. HANNAH: Yes. Sorry, Your Honor.

BY MR. HANNAH:

Q. Hypertext Transfer Protocol GET and the Hypertext Transfer Protocol POST that you were talking about in the source code?

A. Yes. We've seen those both in the source code, and in particular in this case you may be, either through the GET or

the POST, you may be providing information to this second network, which would be a problematic.

Q. All right, Doctor. Can we put a check in that box?

A. Yes.

Q. All right. If we turn our attention to the next element, which is the -- it says "apply element". Do you see that?

A. Yes.

Q. Can you explain to the Court what the "apply element" in claim 18 and claim 19, what does that entail?

A. Right. So once you've seen that these met your criteria, right, then you want to apply a is corresponding operator, or in particular an operator that would cause it to drop, where that operator is specified by the one or more packet filtering rules. So this could be a deny -- there are various types of deny, like deny route -- that would cause the packet to be dropped.

Q. If we could look at --

THE COURT: Well, would "drop" as it's used here be the same as quarantine?

THE WITNESS: So quarantine refers to the sort of high-level rule which says I'm going to block certain types of actions, right? Quarantine is something that's passed down and says, okay, I'm going to, as we discussed, change your Scalable Group Tag and there's an associated rule with that tag, right? So the drop is the operator that's specified by that rule, right? So it's saying in this instance if you're trying to

communicate with that network, then we block, right?

THE COURT: But it's a block for that network only, but it might go to a different network?

THE WITNESS: It may. In fact, that's what the patent says and requires, right? You may still -- the quarantine may still allow the user to participate in another network within the company.

THE COURT: Well, or any other network, in theory?

THE WITNESS: Or any other network, yeah. In general the rules could be written and set up however you wanted, but in particular for exfiltration, it may be there are certain parts of the company you can access and certain that you can't. But you're absolutely right, that there are other networks that you can access and some networks you can't.

THE COURT: Well, is that the way the product works? Does the product --

THE WITNESS: Yes.

THE COURT: Do the rules of the product that you say infringe, do they permit the same function; that is, it can be sent to some networks but not to others?

THE WITNESS: Yes.

THE COURT: So the word "drop" would apply to the network who was being blocked?

THE WITNESS: Exactly. And that's why there's a first portion of packets. And here the first portion of packets

refers to those that you do not want to let out; those that you want to block. And we'll see in the remaining claim elements it talks about a second portion of packets that you would wish to allow; that is, there may still be some access that you wish to allow to the user.

So the -- I think you're right on target: There's a first portion of packets --

THE COURT: Well, that's in Paragraph 2 up there.

THE WITNESS: Yes. There's a first and a second portion, and there's a first portion you wish to block and a second portion you may wish to allow.

THE COURT: All right.

BY MR. HANNAH:

Q. So Doctor, let's look back at your animation and let's maybe you can explain it with regard to the --

THE COURT: I understand what that says.

MR. HANNAH: Okay.

BY MR. HANNAH:

Q. So Doctor, I'd like to turn your attention to PTX-1356.

THE COURT: That's in the other book --

MR. HANNAH: Yes.

THE COURT: -- right?

MR. HANNAH: Yes. Yes, Your Honor.

THE COURT: All right. I've got it.

BY MR. HANNAH:

Q. So Doctor, can you please explain what this document is?
A. So this is a document describing the Rapid Threat Containment. That's a way of discussing some of the things we have been talking about. Quarantine is one of the methods used for Rapid Threat Containment. When you notice something is wrong, you limit someone's communication within the system.
MR. HANNAH: I believe this document has already been moved into evidence, Your Honor. Oh, it has not? 1356. So Your Honor, we'd like to move PTX-1356 into evidence.
MR. GAUDET: No objection.
THE COURT: All right.
(Exhibit PTX-1356 received in evidence.)
BY MR. HANNAH:
Q. So let's blow up the first couple paragraphs, and Doctor, can you explain what's being shown here?
A. Sure. As it describes up at the top, "Rapid Threat Containment is the process by which an endpoint can be either isolated or quarantined after having been identified as infected by malware or having been in violation of an established policy in the network."
So this is saying, again, something's gone wrong. In particular you may notice that someone's gathering data which looks like it may be part of an exfiltration attack.
The next paragraph discusses sort of the next step, which is that the quarantine condition is communicated by the Identity

Services Engine. Remember, the Identity Services Engine is part of that DNA architecture, that Digital Network Authorization -- forget what the "A" is. The DNA architecture.

THE COURT: Which includes StealthWatch, right?

THE WITNESS: Which includes StealthWatch, absolutely. And includes this Identity Services Engine.

A. It then says that the ISE, the Identity Services Engine, communicates a change of authorization within the network device to which the endpoint is attached, right? So it's saying, look, we're going to send information down saying that there's been a change of authorization; that now this endpoint, this user no longer is able to access the entirety of the network depending on the rules set up. And that this is, if you look at the end of this paragraph, that's communicated to the network device by the downloading ACL. And remember, ACL is Access Control List. I showed some code about Access Control Lists. That's how it enforces rules like don't send it to this network, or a Scalable Group Tag. So that's with the SGT we've been talking about being assigned to the interface or associated with the endpoint, respectively, right? So that's saying, okay, we're now going to look more closely at information going in or coming out of this endpoint, and there's going to be new special rules to try and keep them from accessing certain parts of the network.

And it says here in the next paragraph, "These downloadable parameters should then limit that endpoint's ability to

communicate in the network."

And then as you've pointed out, this is all part of "Connected through StealthWatch." And it says, you know, as it says in the next sentence, when we say quarantine, it really infers one of two actions after a policy violation in StealthWatch. So that's what we were discussing before with both the deposition testimony and in the code.

BY MR. HANNAH:

Q. All right. If we can go to PTX-1326?

Doctor, what is -- well, hold on.

A. This is a document related to the Cisco Identity Services Engine. It's an ordering guide. So I'd assume that would be available for public consumption.

MR. HANNAH: Your Honor, we'd like to move PTX-1326 into evidence.

MR. GAUDET: No objection.

THE COURT: That will be admitted.

(Exhibit PTX-1326 received in evidence.)

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. So if we go to Page 11 of this document?

MR. HANNAH: And, Your Honor, it has the same corresponding Bates number, which is 0011.

THE COURT: Okay.

BY MR. HANNAH:

Q. If we look under 1.6 and kind of blow that up?

Doctor, can you explain what's being shown here when it's talking about the Rapid Threat Containment?

A. Sure. So again, the Rapid Threat Containment says "Makes it easy to get fast answers about threats on your network and to stop them even faster." And again, it uses -- or it's based on the network control using Cisco ISE. That's the Identity Services Engine. That's what we've been discussing. And as it says here, "Using this, you can manually or automatically change your user's access privileges when there's suspicious activity, a threat or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications." And that's just another way of saying that there may be places inside or outside to external networks where you're going to allow the user to still work and function but there may be other parts where they're not allowed.

Q. And Doctor -- and this is, in other words, is this showing how the switches and the routers will block traffic automatically?

A. Absolutely. This shows that it can automatically block traffic when a threat is discovered.

THE COURT: Well, this means that if your end user was, for example, a corporation and was a separate network, that you could allow some information to go to the corporation and

other information not to go to them that was generated from the same source?

THE WITNESS: So the way typically the policies are instrumented is you restrict according to source and destination. So you would say, well, I'm not going to let you reach out to this other location, to this other network, right, and it will block sort of that -- it will block the communication between you and that other network.

THE COURT: Well, in other words, if Cisco was sending this information to Centripetal, Centripetal, for example, the program would stop the source code from going to Centripetal, but it wouldn't stop the white papers from going to Centripetal?

THE WITNESS: Well, so the --

THE COURT: If it had the same source and the same end user, but I suppose if they were doing that in real life, Cisco would encrypt the source code.

THE WITNESS: Typically when you do this sort of blocking, you have to block the whole connection because it's very hard if the communication is encrypted or the communication could be hidden in some way, you know, if you allow out communication, you can't always be sure exactly what's in the communication. So it makes sense what you're saying, that if Cisco was concerned about its source code being sent to Centripetal, right, if it noticed some unusual activity, what it would do is say, well, you can't send stuff out to Centripetal's

network; on the other hand, you can still look at Centripetal's web pages out on the open web.

THE COURT: All right. So the technology is not able to permit white papers to go from Cisco to Centripetal, but block source code to go from Cisco to Centripetal?

THE WITNESS: In the case where you're blocking network connections, that's what you'd be able to block, is you would say this user cannot send out information out to the Centripetal network, but out on the open web, as long as it's just accessing web pages, that may be allowed to go through.

THE COURT: Well, of course there would be no reason for them to send the source code. That's not a good example, because they wouldn't be sending the source code, encrypted or otherwise.

THE WITNESS: Well, if you had an exfiltration, right, if you could imagine a Cisco employee trying to make money by taking stuff, Cisco source code out, that would be the sort of threat that Cisco would want to protect against.

THE COURT: Yes, that would be an internal exfiltration situation.

THE WITNESS: Exactly. That would be someone on the inside arranging an exfiltration. It could also be unaware. It could be some malware code that's doing it as well. So it doesn't have to assume that there's a bad person inside for this to happen.

THE COURT: Well, let's move on. I don't need an answer necessarily to a hypothetical question. Go ahead.

BY MR. HANNAH:

Q. Okay. And maybe it'll help just to kind of round this up. If we turn back to PTX-563 and look at the page ending in Bates No. 415. This is the diagram we showed earlier.

So Doctor, could you explain this diagram again and show how the exfiltration works and how that would protect against it with the Rapid Threat Containment?

A. Right. So this is saying, for instance, that you had, that you had a supplier and you changed their authorization so they were quarantined, and you would say, well, they're no longer able to access any of the internal important information, things like potentially the source code, but they're still allowed to go out and, say, access the Internet, because that on its own should be a harmless endeavor that they may need to do to do their normal run-of-the-mill work.

Q. So if we look at this diagram where it prevents the high-risk segment, that could potentially be housing the source code of Cisco and this would block the suspected computer from accessing that protected network; is that right?

A. Yes. A different part of the network, yes.

Q. That would prevent that exfiltration?

A. Yes.

THE COURT: All right.

MR. HANNAH: May I move on, Your Honor?

THE COURT: You may.

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. If we could go to PTX-1280? If we go to Page 21? This document's already been admitted.

And if we look at the bottom, Doctor, can you identify the specific operator that's going to be applied in order to prevent this exfiltration from happening?

A. All right. So this discusses or explains that it would limit the network access, and this would be done, you can see at the bottom, it talks about permissions. You know, it says from group 255 quarantined systems to the development servers, it says those will be denied. So those communications will be denied.

Q. So that's being shown with the "deny IP" as shown on the document?

A. Yes. I interpret these deny IPs are showing that there are certain communications that are going to be dropped, not allowed, based on the groups corresponding and can be based on the corresponding networks that these groups belong to.

Q. Thank you, Doctor. I'd like to turn your testimony -- turn your attention to the testimony of Peter Jones. And this is found at Page 30, Line 23 through Page 31, Line 20, and can you explain what Peter Jones is --

THE COURT: All right. Well, how is this slide marked that we're going identify?

MR. HANNAH: We can submit it to Your Honor with a PTX number, and we can do that for all the slides that we use.

THE COURT: All right. This is Peter Jones. I want to make sure that we have these slides, and at this point only these slides, from these depositions admitted.

MR. HANNAH: We'll do that, Your Honor. We'll assign PTX numbers to each of these slides and we can read those into the record tomorrow, and then we will also have all of the slides ready to go for tomorrow so we can --

THE COURT: All right. Well, let me read this. UADP in particular. What is -- let me look up UADP.

THE WITNESS: That's Unified Access --

THE COURT: No, it's not on the list. What is UADP?

THE WITNESS: Unified Access Data Plane. That's the processor that's inside the switches and routers. That's the processor that processes the packets. That was that special processor that's its own specialized hardware that we had talked about.

THE COURT: Unified Access Data Processor?

THE WITNESS: Data Plane, I think.

THE COURT: Data Plane. P-l-a-n-e or --

THE WITNESS: Yeah. Data plane is like the level, or where the data is going through.

THE COURT: All right. Let me try to read this.

THE WITNESS: I can highlight for you the part that's most important at the bottom when you feel ready, Your Honor.

THE COURT: Okay.

(Pause in the record.)

"Send them to a TCAM." I don't know what that is.

THE WITNESS: I can explain that too if it's not on the list.

THE COURT: Ternary Content Addressable Memory. Okay.

(Pause in the record.)

THE COURT: Well, that's better than the last one I looked at, but I'd like to still like to hear your explanation.

THE WITNESS: Sure. So what it's saying is remember we said that that UADP, Unified Access Data Plane, that's a processor, and it's sort of a special processor. One of its primary functions is when a packet comes in, it's supposed to look at that packet and figure out where it's supposed to go out, okay? And beyond where it's --

THE COURT: Based on the header?

THE WITNESS: Based on the header and associated information. Exactly.

And as part of that, it may also figure out that it's supposed to just drop the packet, supposed to not send the packet on at all. So the first paragraph, all it's really saying is, you know, packet comes in, we have to look at it,

process it, and figure out what to do with it.

And then if you look at the bottom starting at the associated data, or even before that, I will then go and -- okay yeah. Let's just undo that one sec and I'll read the last sentence.

"The associated data will include multiple fields, including such things as a deny route." Okay. That's just saying after this processor is all done, it's going to send you back information; that information may be where to forward the packet, but in some cases the information will be, yeah, don't forward that packet at all, just drop the packet.

And now if we can bold that last part, right, that's really what we're saying, or the main point of this quote, is it says "Deny route says that you drop." You would then drop the packet. Or you would refuse to forward the packet to layer 3. That means, you know, refusing to forward is dropping.

It might also do deny bridge, which means you would refuse to forward it to layer 2.

So one is more used in routers, one is more used in switches, both of them have a deny operation, and deny, here again, means to drop the packet.

So all this is deposition testimony saying what we had seen in the documentation before, that one of the purposes of these routers and switches, it looks into these rules, it looks into these rules based using things like the UADP, and based on

that rule, it may decide, well, I have to drop the packet for security reasons.

THE COURT: Well, when you said earlier header and associated information, associated information might be quantity of the transmission or the header would have the source and the recipient?

THE WITNESS: Right. So the --

THE COURT: You say associated information, that may be like the volume of the transmission?

THE WITNESS: Well, in particular here -- that could be. But in particular here, what I was really thinking of was remember that Scalable Group Transmission Tag? That SGT tag? So sometimes rules depend on that tag. And remember, we've said some packets have been tagged, and based on that tag they're sort of treated differently? They get extra rules, right? So that would be -- the associated information that's in the header is the Scalable Group Tag.

THE COURT: In other words, they only go to people in Group 1 through 3, they wouldn't go to people in Group 4 through 6?

THE WITNESS: Right. That might be -- and it might be the same that you can only go to these other groups, or in particular it might also be you can only go to these networks or parts of the network.

THE COURT: Okay.

BY MR. HANNAH:

Q. All right, Doctor, if we could go back to the claims.

Do the Catalyst routers and the ISR and ASR -- I mean the ASR and ISR routers and the Catalyst switches, do they meet the "apply element" as found in both 18 and 19?

A. Yes, they do.

Q. And can you just give us a little recap as to why?

A. Right. Again, so here the first portion of the packets would be packets that meet the security rule that are being told you can't go to this network because you're now a potential security threat. So again, that's specified by the one or more packet filtering rules. And as we've seen, it can be configured to drop the packets associated with that type of transfer.

Q. And is the drop -- is that the deny route and the deny bridge that we just saw on the documents in the testimony?

A. Yes. Can also be referred to as deny route or deny bridge are ways of, that drop is implemented.

Q. Can we check that box?

A. Yes.

Q. If we go to the next element, which is simply "drop each packet in the first portion of the packets." Do you see that?

A. Yes.

Q. Do the Cisco routers and switches, do they drop packets?

A. Yes, they do. And according to the rules, they would drop each packet in the first portion of packets like we've

described.

Q. If you turn to PTX-1390?

Can you explain what this is, Doctor?

A. This is, again, another outward-facing Cisco document describing some of their technology.

MR. HANNAH: Your Honor, we'd like to move PTX-1390 into evidence, please.

MR. GAUDET: No objection.

THE COURT: All right. That will be admitted.

(Exhibit PTX-1390 received in evidence.)

MR. HANNAH: Your Honor, we'd like to turn to Page 86 of this document. It ends in page Bates No. 86. 0086.

THE COURT: All right.

BY MR. HANNAH:

Q. If we look at the second bullet point, Doctor, can you explain how this informs your opinion as to whether the "drop the packet" limitation is met?

A. So it says here, "a packet is dropped if it hits the deny rule in any of these types of ACLs." ACLs is Access Control Lists. Again, the ACL is the rule that says, okay, we're going to potentially drop this packet. All this occurs, again, within the, within the router or the switch as we've described. And again, this just shows that it can drop packets or deny based on these security rules that we've described.

THE COURT: ACL means...

THE WITNESS: Access Control List.

THE COURT: Right.

THE WITNESS: It's like you can think of ACL, it might be easier mentally translated as like rules.

THE COURT: Right.

BY MR. HANNAH:

Q. If we go back to PTX-1276, which has already been admitted into evidence, and turn to Page 216, which we've seen before, if we blow up the figure, can you explain to the Court how this informed your opinion with regard to the dropping of packets limitation?

A. I always just liked this picture because I think it just makes this very clear: A packet comes in, has to go through all these various steps, various checks from these ACL list of rules, and at various places if it doesn't pass, the packet will get denied, which corresponds to a drop as shown in the center.

THE COURT: Would the left-hand side of this chart be Level 2 and the right-hand Level 3?

THE WITNESS: I don't believe so. If I'm reading it right, my recollection is that it breaks up the rule sets into two parts. It sort of looks at it sort of coming in based on the information when the packet comes in, and then it does a lookup to figure out, you know, what's actually going -- where the packet's supposed to go, and then on the right-hand side has to do with rules for where it might be going out.

BY MR. HANNAH:

Q. And Doctor, this is a just as a reminder, this is the flow diagram for the operating system for both the switches and the routers; is that correct?

A. Right. Both the switches and the routers.

Q. So Doctor, if we turn back to the claims, do the switches and routers, do they meet the limitation in both Claims 18 and 19 that says "drop each packet in the first portion of packets"?

A. Yes, they do.

Q. Can we check that box?

A. Yes.

Q. All right. Let's turn to the --

THE COURT: I didn't hear the answer to that question.

THE WITNESS: Oh, yes. Sorry. Check the box.

THE COURT: Okay.

BY MR. HANNAH:

Q. So if we could turn to the next element, Doctor, can you explain the --

A. The next element --

Q. Go ahead, Doctor.

A. Oh. So I think -- and correct me if I'm wrong -- for the next, we sort of have these next three elements and we're sort of taking them together, and because really, this is just the opposite side or the other side of what we had talked about, which is that there are some packets, right, that you might say,

well, those have got to get dropped because they're going to a part of the network that's now a security threat. But now there are other packets, a second portion of packets going to some other network that are perfectly fine, right? So as opposed to having drop conditions here, here we have forward conditions. So it says "responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria," so these packets are okay, that they aren't violating the rule, and that these "wherein the data indicates that the second portion of packets is destined for a third network." That is, the reason they're okay is because they're going to a safe network as opposed to a -- to a permitted network as opposed to an unsafe network. Then you apply to each of those packets in the second portion without applying the packet filtering rules that would cause you to drop in the first portion; that you would now use an operator configured to forward those packets to the network.

So it's really just, you know, the other side of the coin for what we had been talking about before: Some things you would want to block, other things you would want to allow.

Q. And then if you could, just for the record, explain what is shown in the last element for both Claims 18 and 19?

A. For both claims 18 and 19 it says you then forward each of those packets and the second portion of packets toward the third network.

Q. And are the second -- this is the second "responsive to" element and the second "apply" element, and this "forward" element, are they identical for claims 18 and 19?

A. Yes.

Q. And does the same evidence that we've been using for the routers and switches, does it also apply for the routers and switches in regard to each of these elements?

A. Yes.

Q. Doctor, I was going to take you back to your demonstrative but I'm not sure if the Court wants to see that again, so we'll skip on that one.

Let's go to PTX-563 which has been admitted. This is the same diagram that we've seen before, Page 120.

Can you just explain for the record how this demonstrates that the second "responsive to", "apply" and "forward" elements are met as you stated that are the other side of the coin and where that's shown on this figure?

A. The way I see this figure is with that green check is saying that while this supplier has been quarantined and so therefore cannot access certain other networks internal to the corporation that might include things like high-risk segments or employee information, they're allowed to go out to another network, out on the Internet, you know, for instance to wherever Google is or something, and do searches may still be allowed because that might be considered a part of their normal work.

THE COURT: That would have to be their web page, right?

THE WITNESS: Yeah. They might need their web pages. So that just shows, again that, according to this determination, you may still forward packets out to a third network under this system.

BY MR. HANNAH:

Q. You anticipated my question. Is that the, as shown in this diagram, the third network where the packets are allowed to is the Internet with the green checkmark; is that right?

A. Right. That would correspond to parts of the Internet, yes.

Q. And as we said before, the red boxes indicate the second network which the computer would be prevented from accessing; is that correct?

A. That's a yes. That's what the figure shows.

Q. I'd like to show you PTX-1288. Can you explain to the Court what this document is?

A. All right. So we have talked about ACLs. You can see that in the title here. Security Access Control Lists. So these would be, again, Access Control Lists related to security. These are the way I would describe them again as the rules setup that either prevents certain packets from going to where they want to go or allowing them to go where they want to go.

MR. HANNAH: Your Honor, we'd like to move PTX-1288

into evidence, please.

THE COURT: That will be admitted.

(Exhibit PTX-1288 received in evidence.)

BY MR. HANNAH:

Q. Doctor, if we go to Page 12 of this diagram -- I mean of this document?

MR. HANNAH: And Your Honor, it's on Page 0012, the same corresponding Bates number.

BY MR. HANNAH:

Q. Is this a similar diagram that we've been talking about with regard to the flow on the switches and the routers?

A. It's the same sort of thing. Some things that are useful to see specifically in this figure is, if you look at the title of the figure, as it says it's a typical security ACL application on a packet. So this is saying that this is an Access Control List, and it's part of the goal of security.

And the other thing is just you can see the "Permits" all around. I hadn't pointed them out before, you know, but you keep permitting, permitting until you get to the packet goes out, and the packet goes on that corresponds to the forwarding that is required by these parts or these claim elements. And you can tell that the packet goes out corresponds to forwarding, there's a forwarding lookup that says we're doing a forwarding lookup trying to determine where the packet should be forwarded, where it should go toward the third network, and then the packet

will go out if it's not denied.

Q. If we turn to the next page in this document, which is Page 13?

MR. HANNAH: Your Honor, it's also 0013 for the Bates number.

BY MR. HANNAH:

Q. If we can just show the bottom, 4.1? Yeah, blow that --

Can you explain how this informed your opinion, and specifically with regard to the permit and the deny which is being shown here, and how that maps to the forward and the drop of the claims.

A. All right. So what this is saying is that you can create these Access Control Lists, and these Access Control Lists, you can think of them as having, you know, sort of in subparts where it tells you what's permitted and what has to be denied. And this is just providing to someone who is familiar with these sorts of structures, you know, what these rule lists, what they look like. But for us, the key issue here is that these actions, two of the main actions are Permit, which means allow or forward on, or Deny, which is drop.

Q. All right. Thank you, Doctor. I'd like to turn your attention to the deposition testimony of Peter Jones. And we have a slide for that.

MR. HANNAH: And Your Honor, we will mark this slide as a PTX number and submit it.

THE COURT: All right. Let me have a chance to read this first.

MR. HANNAH: Of course.

(Pause in the record.)

THE COURT: Okay.

BY MR. HANNAH:

Q. Doctor, could you please explain what's being shown here?

A. Sure. So he's being asked about how, again, this sort of forwarding of packets works. And he's asked to describe it in layman's terms, and he says this is how you would set up the rules, is really what he's saying, okay? So he says let's imagine them all going toward you I want to throw away, all of them going toward someone else I want to permit or to forward. I'll put an entry, right, I would create a part of that rule that matches your address that says anything going to you I'm going discard it, right? So the first rule on the list is if it's going to the person I don't want it to go to, it's going get dropped and thrown. Then I can have a rule that says, well, everything is fine, it can go where it's supposed to go, so everyone else will be a match entry. I can do that with two single entries, one matches you, one which matches everything.

So the idea is exactly here what we were saying: You can set up the rules to say, hey, if it's trying to go to this network -- and it doesn't have to be just one network, it could be a collection of networks -- you could say, well, if it's

trying to go to one of these bad places, it's going to get dropped, and if it's going to a good place or a place that's not one of the bad places, it will be okay. And you can set it up with explicit actions, like here is a list of good places it can go, or you can just say, well, there are good places it can go and there are bad places, and if it's not one of the bad places, then it's always okay. You can do these sort of default rules as well.

But the key is that, just as we've seen there are rules that can be used to block or deny things, you set up rules to allow things, to forward things on to other networks if you want.

THE COURT: Well, I guess you could do the inverse, and you could just say it can only go these groups and nobody else?

THE WITNESS: You could do that as well. Absolutely.

BY MR. HANNAH:

Q. All right. Doctor, I'd like to show you another piece of testimony. This is from Martin Hughes. This is at Page, for the record, at Page 40, Line 9 through 40 at Line 19.

MR. HANNAH: And before I ask any questions I'll let Your Honor have a chance read it if you like.

(Pause in the record.)

THE COURT: Okay.

BY MR. HANNAH:

Q. So Doctor, can you please explain for the Court what this is showing in terms of how this maps to the forwarding element in claim 18 and 19?

A. All right. So both the claims call for the devices, the switches and routers, to forward packets, and this is saying something, you know -- or quite clearly showing that, in fact, yes, these devices forward packets based on the corresponding rules and structures. In a more technical level, what it's saying is that there's a part of the operating system that's set up to manage and control the internal computer structures that decide whether things are going to get forwarded or whether they're going to get dropped and how they're going get forwarded if they're forwarded. And so it refers to that as the forwarding manager.

The high-level point to take here is that naturally these devices forward packets.

Q. All right. Thank you, Doctor.

If we turn back to the claims, can you give us a recap in terms of how each of these limitations of both Claims 18 and 19 are met by the Catalyst switches and the ASR and ISR routers?

A. Right. So again, we've seen, one can understand from like this exfiltration example, maybe, that you don't want to let data out to a potentially dangerous place, but I'd still like the user able to, say, interact with the Internet or interact with our safe places. So you could be looking at this second

portion of packets and determine that it does not correspond to previous criteria, the criteria that would cause it to be dropped, and in particular where that criteria would correspond to the fact that it was headed to a third network, a safe network instead of a second network, a dangerous network. So we're responsive to that determination, or we've shown that devices are responsive to that determination.

We've shown that they apply in the second portion of packets without applying those packet filtering rules that prevent that type of data transfer.

A second operator. And the operator here is going to be the forward operator, the allow operator, sometimes, or we've seen it also referred to as permit. And that would forward packets not associated with the particular type of data transfer towards the third network.

And then, you know, the operator of course is designed to forward the packets, and then it will actually, as in the last part of this claim element, actually forward each packet in that second portion of packets toward the third network.

Q. So Doctor, can we check those boxes?

A. Yes.

Q. If we turn to the next slide, there's an overall recap. Is this just a recap of all of the testimony that you've provided today with regard to how the routers and switches infringe the '193 patent?

A. Right. This is a high-level description showing again that we meet all the individual claim elements and summarizing how each of those claim elements are met.

MR. HANNAH: I'll just give the Court a second to read this if you'd like.

(Pause in the record.)

THE COURT: All right.

MR. HANNAH: Your Honor, did you have any questions? We were going to move onto the doctrine of equivalents with this patent.

THE COURT: No, I don't have any questions.

MR. HANNAH: Thank Your Honor.

BY MR. HANNAH:

Q. So Doctor, let's turn to the doctrine of equivalents. Can you explain what is your opinion with regard to the doctrine of equivalents with respect to the '193 patent?

A. First, to begin, let me state clearly that I believe that there is literal infringement; that there's infringement without the doctrine of equivalents. However, I know that, you know, the Cisco attorneys and experts are going to try and present their own take or cast doubts on those opinions. And in particular, I'm aware that they seem to have some issue or discussion with the first "responsive to" limitation that we've gone over, in particular issues relating to, you know, whether these setups are designed to actually prevent certain types of

data transfers. And so because of that, I also wanted to offer a doctrine of equivalents analysis or framing as well.

And in the past when I've done doctrine of equivalents I've used the Substantially Same test as one of the ways or descriptions I'm aware of that you can provide. The doctrine of equivalents involves saying it performs substantially the same function substantially the same way to obtain substantially the same result.

Q. So can you explain for the Court why, in your opinion, that while we understand at the very least, while we understand at the very least that the first "responsive to" element is met because it performs substantially -- the Catalyst routers and the ASR and ISR routers and the Catalyst switches perform substantially the same function as the first "responsive to" element?

A. Well, the first "responsive to" element is to, based on rules, stop certain types of data transfers from occurring. And that function is met by the Cisco products through the use of the security infrastructure, the security tag -- or Scalable Group Tag, sorry, and the security Access Control Lists that we've discussed. It performs substantially the same function of making sure that traffic that may be headed towards a specific network that is going to be denied, and again, that that comes about because of certain types of traffic that it's trying to stop.

Q. Can you explain how the products are made -- or meet the element in substantially the same way?

A. So as discussed in the claim element, that the way that this is accomplished is to use an operator that's meant to drop certain packets, in particular the first portion of packets, and as we've seen, that's what it does through this deny route or deny bridge or in general just the deny mechanism, and that these operators make sure that the packets are dropped so that they don't go to the unsafe second network.

Q. Can you explain how the Catalyst switches and the ASR and ISR routers meet this element and achieve substantially the same result?

A. Achieve substantially the same result because, again, the collection of first packets are stopped -- or dropped, I should say, based on the corresponding rule and operator -- rules and operators and, you know, for this claim element. Of course we see the same results that the packets for that second network are dropped. And of course throughout the patent we also see the same result that packets destined for other networks can be allowed to proceed.

MR. HANNAH: Thank you, Doctor.

Your Honor, at this time we'd like to move to the '806 patent.

THE COURT: All right. Let me see that last slide.

(Pause in the record.)

THE COURT: All right. You're moving to the '806 patent now?

MR. HANNAH: Yes, Your Honor.

THE COURT: All right. Is this a different book or what?

MR. HANNAH: No, it should be the same book, Your Honor.

THE COURT: Okay.

MR. HANNAH: But there is an additional product, so we have the switches, the routers and now we also have the firewalls for the '806.

THE COURT: This is the rule swap --

MR. HANNAH: Correct, Your Honor.

THE COURT: -- patent? Okay.

MR. HANNAH: Your Honor, in terms of the presentation of evidence, we intended to -- we'll go through Claims 19 and 17 in a similar manner in that they are going to be side-by-side since they're very similar, and we'll go through both of those through one pass for the routers and switches because they have the same operating system, and then we're going to do another pass with the firewalls and show the proof of infringement for those.

THE COURT: All right.

BY MR. HANNAH:

Q. Since we haven't talked about the firewalls, I'd like to

show you, Dr. Mitzenmacher, I'd like to show you, it was Slide 15 that we kind of skipped over earlier.

Thank you, Geoff.

Can you tell us for the record when we refer to Firepower firewalls or the firewalls or the Adaptive Security Appliance, what are we referring to?

A. So we're referring to these sets of products, the 1000 series, 2100 series, 4100 series, 9300 series and the Cisco Adaptive Security Appliance, the 500X with Firepower Services. These are the firewall products, and you've heard discussions of firewalls I believe at great length in the tutorials and how they're used to protect networks.

THE COURT: Well, the firewalls are not themselves -- or this isn't actually marked as an exhibit, right?

MR. HANNAH: This is not, Your Honor, but we have -- we will have other exhibits that show the actual model numbers that we're talking about.

THE COURT: Okay.

THE WITNESS: This is just a summary.

MR. HANNAH: Yeah.

BY MR. HANNAH:

Q. And Doctor, is it fair if we refer to the firewalls that we're -- for the purposes of your testimony, we're referring to both Firepower firewalls and the Adaptive Security Appliance, which is also known as the ASA, and both those with the

Firepower Management Console; is that correct?

A. Yes. We'll be talking about these sets of firewalls, and we'll also be talking about the Firepower Management Console which is something used to control the various Firepowers or collections of firewall devices.

THE COURT: Why are these referred to as next-generation firewalls?

THE WITNESS: I believe that I'd say they're called next-generation firewalls precisely because they contain a number of new and advanced security features, including I think some of the security features that are discussed in this case, both in probably my patents and with my, I understand the other patents being handled by the other experts.

THE COURT: By the next-generation, are you saying that these were developed after the '806 patent? Is that what you mean by next-generation?

THE WITNESS: No, I believe next-generation is, like you can actually see it if you look in the 4100, if you blow that up on the right, Geoff, I don't know if you can get that, the 4100 you can -- yeah, if you can blow that up you can see --

MR. HANNAH: He's not going to be able to blow it up. It's a PowerPoint.

THE WITNESS: Okay. Okay. So it's very hard to read. I can just make it out on my screen. But for instance, under the 4100 it says "Stop more threats with our fully integrated

next-generation firewall (NGFW)."

Similarly for the 5500, if you look at it says, you know, there it's a bit bigger, it says "Stop more threats with the threat-focused 5500X NGFW", where that stands for next-generation firewall. And one could say this is something of perhaps a marketing term, but it's something Cisco at least I've seen uses, and I would understand that as referring generally to much more advanced or more advanced security considerations that have been embedded in their latest products.

BY MR. HANNAH:

Q. Doctor, let me show you a data sheet which you should be able to read it a little bit easier, which is PTX-1883.

Doctor, can you explain for the Court, what is this document?

A. So this is another data sheet. Here it's a data sheet for the Firepower appliances generally.

Q. If you blow up the first paragraph, I believe this is what you were trying to read when it's talking about the next generation firewall.

A. Right. So "The Cisco Firepower NGFW or next-generation firewall is the industry's first fully integrated threat-focused next-gen firewall with unified management. It uniquely provides advanced threat protection before, during and after attacks."

This is, I think, something, you know -- next-generation firewall is a term used a lot, but one of the things that I

think highlights it in much of the literature is this idea it's offering more advanced threat protection, but in particular before, during and after attacks, which may be an emphasis on before, whereas the idea is you're trying to stop things before they happen.

MR. HANNAH: Your Honor, I'd like to move PTX-1883 into evidence, please.

MR. GAUDET: No objection.

(Exhibit PTX-1883 received in evidence.)

BY MR. HANNAH:

Q. Doctor, if we could go to the second page of that document, does this, does the second page of this document show the various series of appliances that we'll be talking about and list them?

A. Yes. So this matches our previous slide in terms of the families of products, 1000 series, 2100 series, 4100 series, 9300 appliances, and the 5500. The ASA 5500.

THE COURT: Are these products that you say infringe?

THE WITNESS: The products in these, this collection of products, all of these.

BY MR. HANNAH:

Q. It's each of these products; is that right, Doctor?

A. Yes. Each of these products.

THE COURT: All right. So this is a list of the products which you're prepared to say infringe --

THE WITNESS: Yes.

THE COURT: -- the six patents; is that right?

THE WITNESS: The '806 patent, and I'll later be talking about them with regard to the '205 patent as well.

THE COURT: All right. Let me write these down.

(Pause in the record.)

THE COURT: All right.

MR. HANNAH: Thank you, Your Honor.

BY MR. HANNAH:

Q. Doctor, if you could look to the second line of the paragraph that's shown, and can you explain what it means that the Cisco Firepower Management Center software is on each of these appliances?

A. Yes. So in particular, as before, when we were talking about the switches and routers, you know, there we were talking about sort of the underlying operating system. Here we're talking about all these appliances are running the same essential software image, the Firepower Management Center software image. And so the reason that we're able to view all these products together is because they're all using the same software base.

Q. All right. And if we go -- if you take that down, Geoff, and go to the second paragraph below, Cisco Firepower Management Center?

A. Yes.

Q. Is this the Firepower Management Center that we mentioned earlier that interacts with each of these firewalls?

A. Yes. So the Cisco Firepower Management Center that you're highlighting there provides centralized management of the Cisco Firepower NGFW. Essentially you can run a number of different Firepower devices through a single management center. In this way you can make the analogy or liken it to the fact that the -- remember there was the DNA Center, the Digital Network Architecture Center which would help manage or run checks of routers and switches, including help manage the security rules and security setup or posture setup on those devices. And we have the same sort of framework here in that there's a management center that can be used to manage or deploy rules and so on to a family of Firepower devices.

Q. All right. Thank you, Doctor.

Now, earlier you testified that there was some additional security that was added to these firewalls in order to make it a next-generation firewall. Was one of those technologies the Threat Intelligence Director?

A. Yes.

Q. And if we can look at PTX-519?

Can you explain what that document is and what it's explaining?

A. My understanding is --

THE COURT: I'm sorry, where are we now? What?

MR. HANNAH: PTX-519, Your Honor.

THE COURT: Okay.

BY MR. HANNAH:

Q. So Doctor, we heard -- Dr. Moore last week said that Centripetal helped coin the phrase operationalizing threat intelligence. Is this article that we're seeing in PTX-519, is this talking about the same type of operationalizing threat intelligence?

A. Yes. In fact, if you look at the top or at the title you can see that exact same phrase where it's talking about the plan or approach to operationalizing threat intelligence.

MR. HANNAH: Your Honor, we'd like to move PTX-519 into evidence, please.

THE COURT: That will be admitted.

(Exhibit PTX-519 received in evidence.)

MR. HANNAH: If we go to the second page of this document?

For Your Honor's convenience it ends in Bates No. 831.

THE COURT: Okay.

BY MR. HANNAH:

Q. And we'll blow it up from -- well, I guess under the second paragraph, talk about it from there, and then down to the diagram as well.

Can you explain what's being shown here in terms of how Cisco operationalizes threat intelligence?

A. Sure. So you can see different sorts of flows in the picture going in to the Threat Intelligence Director, which is on the Firepower Management Center, okay, and as it says, the Threat Intelligence Director operationalizes cyber threat intelligence. I believe that's what Dr. Moore was talking about an awful lot last week. And again, this is, I think, one of the main parts of next-generation firewalls, is the idea you try and stop some number of things before they get to your network. So what it does is it takes open industry standards for threat information -- you'll see the acronym STIX and TAXII. I'm going to have to look those up for you because I can never remember them off the top of my head. I have them written down somewhere if you'd like. But you can think of them as these are just threat intelligence feeds. These are information coming in from the Cloud, into the appliance, and it's using that information to say, a-ha, based on this information -- as well as you can see on the right-hand side information it's gathering internal to the network itself through its Cisco security sensors -- let's take all this information and figure out how to update our rules, how to manage, how to make sure that we are blocking what we need to be blocking hopefully before it actually hits our network, okay?

So if you can look, there's a line there that says "Intelligence director can easily ingest third-party threat feeds and data from threat intelligent platforms." I can point

to it or if you can see it -- right.

The Threat Intelligence Director can easily ingest third-party threat feeds and data from threat intelligent platforms to your network sensors and next-generation firewalls. Based on your confidence in this additional intelligence, you can direct your network sensors to use it to automatically monitor or block traffic inline."

So the idea here -- and this is hopefully an idea that you feel more familiarity with over the last week or so -- is that your management device is getting all the sort of threat information based on external sources in some cases, based on this threat intelligence, and it's taking it and it's saying, okay, we need to come up with new rules, new approaches, toss them down into the network and tell them, look, you need to block this traffic, or in some cases perhaps monitor this traffic just to make sure that we are blocking threats, new threats, or at least seeing new threats as they arise.

THE COURT: Well, what is the advantage of blocking these threats through firewalls as opposed to through switches and routers?

THE WITNESS: Right. So that's a great question. So I think we talked about this last week, the importance of a layered defense. Of having multiple layers of security. Because you can never tell when some piece of malware or some bad code or bad packet is going to sneak through one of your

layers, and then you want to have additional layers that are prepared to stop it. So part of the reason is simply that you'd like to have multiple layers of security in case one of your layers of defense gets broken through, hopefully another layer will be able to stop it before it reaches your end machine.

Another reason -- oh, sorry. Go ahead.

THE COURT: Where would the threat intelligence platform get the threat intelligence that the switches and routers couldn't also get?

THE WITNESS: So you can pass some of that information down to all of them. Sometimes there's different sorts threats that certain devices may be better equipped to handle, right? Firewalls are generally more powerful, can potentially like deal with a bit more complex issues or interactions. Remember, switches and routers are, in particular, designed to have to be very fast. I mean, as are firewalls as well, but there may be different tradeoffs that you make in terms of putting more expensive resources or more powerful resources at certain points in your system. And there may be, you know, somewhat different or more complex types of structures or functions that can be handled at the firewall that you wouldn't necessarily want to put at a switch or router.

THE COURT: Would it be accurate to say that the firewall specializes in intercepting threats?

THE WITNESS: That's certainly one of the functions.

But the only reason I hesitate with the specializing is, as we've seen, that's been a big push, in particular by Cisco, to push various security infrastructure into the switches and routers as well so that you have this multi-layered, multi-step security system that's both gathering information and providing multiple places where you can stop the threats within your system.

THE COURT: Well, I mean, you said that the firewalls may have more -- a greater ability to recognize threats because they have more power, or what's the right...

THE WITNESS: Yeah. And keep in mind that the routers and switches, besides checking for security, have to do these forwarding functions. Have to figure out where the packets are going to go next.

THE COURT: Well, that's why I asked you the question about specialize.

THE WITNESS: I think I'm finally getting around to your point, maybe. Right. And the firewalls can typically maybe just decide should this packet go forward or not go forward, is it a threat or not a threat, and then let the routers and switches continue to route them. So in that sense, firewalls can have more processing time and more processing power to apply specifically to this task.

THE COURT: But the whole idea is not to slow down the traffic, right?

THE WITNESS: That's right. But they don't have to do quite as much work. They don't have to figure out the routing aspect so they can do more work on the packets.

They may also do things like, in firewalls sometimes you may say, well, this packet is enough of a risk that I'm going to sort of take it off-line and apply additional measures to it. Even if it does delay this packet, that might be okay, as long as the rest of the packets can go through.

THE COURT: All right.

BY MR. HANNAH:

Q. And Doctor, is it your understanding -- and this is for the record -- that the STIX stands for Structural Threat Information Expression?

THE WITNESS: That sounds right. Structural Threat Information Expression? Yes, that sounds right.

MR. HANNAH: Then for TAXII --

THE COURT: Give me STIX again. Is that on my list?

MR. HANNAH: I don't believe it's on your list, Your Honor.

THE COURT: Let me have it again. What does STIX mean?

MR. HANNAH: Structural Threat Information Expression. That's the third-party threat intelligence data feeds.

And then just let me know when you want me to move on.

THE COURT: All right. Move on.

MR. HANNAH: And then TAXII is the Trusted Automated Exchange of Indicator Information. So again, that's the Trusted Automated Exchange of Indicator Information.

THE COURT: Trusted Automated Indicator --

MR. HANNAH: Exchange of Indicator. So like the --

THE COURT: Exchange Indicator.

MR. HANNAH: Information. They have two "i"s.

THE WITNESS: These are not the best acronyms.

MR. HANNAH: They are not.

Your Honor, with that, we're about to turn back to the patent, and it's probably a very good natural breaking spot, or we can continue, whatever Your Honor...

THE COURT: I'm persuaded that it's a good breaking spot.

All right. Is there anything that you need me to talk about in our planning for tomorrow before we adjourn?

MR. HANNAH: Nothing from Centripetal, Your Honor. Thank you.

MR. GAUDET: Nothing from Cisco, Your Honor. Thank you.

THE COURT: All right. Well, we'll be adjourned until 10 tomorrow morning.

(Whereupon, proceedings concluded at 3:59 p.m.)

*CERTIFICATION*

*I certify that the foregoing is a true, complete and correct transcript of Volume 4 of the proceedings held in the above-entitled matter.*

Paul L. McManus, OCR

Digitally signed by Paul L. McManus, OCR
DN: cn=Paul L. McManus, OCR, c=US, email=pmcmanusocer@verizon.net
Date: 2020.08.10 10:29:05 -04'00'

Paul L. McManus, RMR, FCRR

_____

Date